PHYSICAL LAYER SECURITY IN ONE-WAY AND TWO-WAY RELAY SYSTEMS

BY

MOHANAD ALI ABDULWAHID OBEED

A Thesis Presented to the

DEANSHIP OF GRADUATE STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

In

TELECOMMUNICATION ENGINEERING

DECEMBER 2015

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS
DHAHRAN 31261, SAUDI ARABIA

DEANSHIP OF GRADUATE STUDIES

This thesis, written by **MOHANAD ALI ABDULWAHID OBEED** under the direction of his thesis adviser and approved by his thesis committee, has been presented to and accepted by the Dean of Graduate Studies, in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE IN TELECOMMUNICATION**.

Thesis Committee

Dr. Wessam Mesbah (Adviser)

(Co-adviser)

Prof. Salam A. Zummo (Member)

Dr. Maan Kousa (Member)

(Member)

Dr. Ali A. Al-Shaikhi
Department Chairman

Dr. Salam A. Zummo
Dean of Graduate Studies

30/12/15
Date

Dedication

To my Parents, my Wife, sisters, brothers, my son Hossam and my daughter Ragad for their endless support and love.

ACKNOWLEDGMENTS

All praise and thanks be to Almighty Allah, the one and only who helps us in every aspect of our lives.

Acknowledgement is due to King Fahd University of Petroleum and Minerals for giving me this precious opportunity to resume my Master degree.

I would like to express deep gratefulness and appreciation to my Thesis advisor Dr. Wessam Mesbah for his continuous help, guidance, and encouragement throughout the course of this work. He spent a lot of his precious time helping me and advising me with every letter.

Beside my advisor, I would like also to thank my Thesis committee members: Prof. Salam A. Zummo and Dr. Maan Kousa for their great help and cooperation, which contributed significantly to the improvement of this work.

Also, I would like to thank Taiz university that support and encourage me to accomplish this work. Finally, my heartfelt gratitude goes to my parents, my wife, my sons, my brothers, and sisters for their encouragement, prayers, and moral support.

TABLE OF CONTENTS

LIST OF FIGURES

THESIS ABSTRACT

NAME:	Mohanad Ali Abdulwahid Obeed
TITLE OF STUDY:	Physical Layer Security in One-Way and Two-Way Relay Systems
MAJOR FIELD:	Telecommunication engineering
DATE OF DEGREE:	December 2015

Nowadays, physical layer security has attracted significant attention since it can prevent eavesdropping without the help of the upper layer data encryption. The essence is to utilize the channel state information (CSI) of the channels to limit the information rate that can be attained by the unauthorized users (eavesdroppers). In this work, the physical layer security in one way relay system (OWRS) and two-way relay system (TWRS) is studied. In the OWRS, we first minimize the power of relays under information rate constraints. A novel approach is proposed to grant the optimal solution of the non-convex QCQP problem which is much simpler than the semidefinite programming (SDP) approach in terms of complexity. Then it is proved that as the maximum value of the source power increases, the total power

of the relays will decrease. Second, we solve the problem of the secrecy rate maximization by looking for the optimal weight vector of the relays. It is shown that the optimization problem of the beamforming vector is a product of two Rayleigh quotients (RQ) which in general has been considered as a difficult problem. We convert the non-convex problem to a convex problem with one dimension search. Then we significantly simplify the problem using the generalized eigenvalues. In TWRS, in the case of the CSI of the eavesdropper is available, we consider the problem of maximizing the secrecy sum rate under total power constraint. Even though null space beamforming reduced the problem to a product of two RQs, the problem remained hard to solve and suboptimal solutions have been proposed to solve it. Here, two approaches are proposed to maximize the secrecy sum rate: 1) the optimal null space beamforming approach, 2) suboptimal approach (Ignoring one Rayleigh quotient (IORQ)) that outperforms the null space beamforming especially when the number of relays is small. When the CSI of the eavesdropper is unknown, artificial noise is used to impair the signal to noise ratio (SNR) at the eavesdropper. The problem is formulated to reserve the maximum possible power for the artificial noise and a required quality of service (QoS) at the legitimate transceivers are achieved. The problem is formulated as QCQP, and hence the proposed approach adopted in OWRS is upgraded to solve the problem. Our proposed solution can be used for all QCQPs with positive definite objective function and two trace constraints. Simulation results demonstrate the effectiveness of our algorithms in terms of optimality and low complexity.

ملخص الرسالة

الاسم الكامل: مهند علي عبدالوحد عبيد

عنوان الرسالة: الأمان باستخدام الطبقة الفيزيائية في أنظمة المرحلات ذات الاتجاه الواحد والمرحلات ذات الاتجاهين

التخصص: هندسة اتصالات

تاريخ الدرجة العلمية: ماجستير

هذه الأيام نلاحظ ان موضوع تحقيق الأمان باستخدام الطبقة الفيزيائية يحوز اهتمام كثير من الباحثين والمهندسين حيث انه يستطيع ان يمنع التنصت على المعلومات بدون استخدام تشفير الطبقات العليا. خلاصة أمان الطبقة الفيزيائية هو استخدام معلومات حالة القنوات للحد من كمية المعلومات التي ممكن ان يستقبلها المتنصت. في هذه الرسالة درسنا أمان الطبقة الفيزيائية في المرحلات (Relays) ذات الاتجاه الواحد وأيضا في المرحلات التي ترسل في اتجاهين. بالنسبة للأمان في المرحلات ذات الاتجاه الواحد قمنا أولا بتصغير قيمة الطاقة المطلوبة للمرحلات عندما يكون هناك قيود للأمان للمستقبل الشرعي و المتصنت. استطعنا ان نوجد الحل الأمثل لمتجه التوجيه (beamforming vector) حيث ان حلنا أبسط بكثير من الحل باستخدام semidifinit programming (SDP). ثم اثبتنا انه كلما زادت طاقة المرسل قلت طاقة المرحلات. ثانيا قمنا بتعظيم قيمة معدل الأمان (secrecy rate) عندما تكون الطاقة الكاملة محدودة. أوضحنا ان المشكلة هي معضلة (NP-hard) ثم حولناها إلى مسألة قابلة للحل مع بحث عن قيمة معينة ذات بعد واحد. ثم قمنا بتبسيط المسألة باستخدام ال (generalized eigenvalue). أما بالنسبة للأمان في أنظمة المرحلات ذات الاتجاهين فإننا درسنا الأمان في حالة ان معلومة قناة المتنصت متوفرة وأيضا عندما تكون غير متوفرة. في حال توفر معلومة قناة المتنصت قمنا بتعظيم معدل مجموع الأمان (secrecy sum rate) عندما تكون مجموع طاقة الأجهزة محدودة. هذه المسألة تم إثباتها انه مسألة معقدة لكن تم حلها بطريق قريبة من الحل الأمثل والتي تسمى إعدام الإشارة عند المتنصت (null space beamforming) والتي بدورها تم إثباتها أنها أيضا مسألة معقدة. ولذلك نحن هنا اقترحنا حلين منفصلين لهذه المشكلة: 1) إيجاد الحل الأمثل لطريقة إعدام الإشارة عند المتنصت 2) إيجاد حل شبه مثالي عند طريق تجاهل بعض أجزاء المسألة (IORQ) والتي تفوق الطريقة الأولى خاصة عندما يكون عدد المرحلات قليلة. أما اذا كانت معلومة حالة قناة المتنصت غير معروفة فإننا اعتمدنا التشويش الصناعية لتشوية الإشارة عند المتنصت. طريقة حل هذه المسألة هي شبيه

بالطريقة التي تم فيها حل مسألة تقليل الطاقة في المرحلات ذات الاتجاه الواحد. حيث ان طريقتنا يمكن استخدامها لحل كل المسائل QCQP عندما لا يتجاوز عدد القيود 2 وعندما تكون مصفوفة دالة الهدف مصفوفة معرفة موجبة.

CHAPTER 1

INTRODUCTION

Recently, it has become clear that wireless communication systems have a great impact on the way people contact with each other. Wireless communications provide mobility and flexibility which are not provided by wired networks. Wireless systems are also suitable for short-term and quick networks operating for temporary events such as some activities or exhibitions. Besides, wireless networks are developing and prospering very fast without stop which enables them to provide higher rates and be widely deployed to cover wide area. The most important resources in wireless networks are power and bandwidth, where the demand for high information rates that need such precious resources is increasing. Many researchers are working in improving the information rate where many solutions have been proposed, for instance, the relaying schemes, multiple-input-multiple-output (MIMO) antenna technique, cognitive radio and power allocation. Relaying schemes in wireless networks are used to extend the coverage of the wireless networks when the distance between transceivers is long. There are always some

cases that the intended receiver is located out of the range of the transmitter. Therefore, users that are able to receive the transmitted signals can forward the signals that are not intended for them to the intended users. Briefly, in cooperative communications, end users exchange their information through intermediate nodes which in turn receive the signals, decode or amplify them, then forward them to the end users. There are several relaying schemes that signify the job of relays in the system such as compress and forward (CF), decode and forward (DF), and amplify and forward (AF). The simplest relaying scheme is AF as it amplifies the received signal and directs it to the receiver without any processing, detection, or delay. In CF, relays quantize the received signal then forward it to the receiver. The destination needs more information than AF to uncompress the signal, and the relays require higher computational complexity than AF to compress the signal. In DF, relays firstly decode the received signal, encode it again, then forward it to the intended receiver. There are two types of relaying system: one-way relay system (OWRS), and two-way relay system (TWRS).

Since wireless networks are widely spread and used in many applications, the study of security in wireless networks becomes more crucial. There are always cases where some nodes (eavesdroppers) desire to overhear the messages that are intended for the legitimate destination. Consequently, secure communications is an essential issue in wireless communications to protect confidential messages. The goal of secure communications is to receive confidential messages while keeping the eavesdroppers ignorant. That was the reason behind the emergence of

information theoretic secrecy which has recently been considered as an encouraging way to handle the secure communications. In wireless networks, the broadcast and superposition characteristics represent various challenges in guaranteeing secure communications in the existence of eavesdroppers. The broadcast attribute of wireless communications facilitates the eavesdropping while superposition attribute can cause an overlapping of several signals at the destination which enables the eavesdropper to act as a jammer to degrade the signal at the legitimate receivers [1]. Usually, traditional secure communication approaches are built based on a secret key that is controlled at the network layer. The problem in this technique is that the distribution of the secret key in a wireless environment can be observed by unintended users. Additionally, the network layer security is based on the assumption that it is impossible to decode the information signals without the knowledge of the secret key, whereas this is not proven mathematically. The premise of physical layer security is to utilize the artificial noise and the CSI between the legitimate transceivers and source-eavesdropper channel (if available) to limit the information rate that can be attained by an unauthorized user, and keep the quality of the signal at the legitimate receiver acceptable. It is assumed that the eavesdropper has the global knowledge of the CSI of all nodes and has no limit in the resources to decode the information signal. Research in physical layer security can be classified based on the state of the eavesdropper whether he is active or passive. When the eavesdropper is assumed active, the CSI of the eavesdropper can be attained and exploited to minimize the rate at the eaves-

dropper. Whereas, if the eavesdropper is assumed passive, i.e. trying to hide his presence by not participating in the transmission, the appropriate way is to emit a jamming signal in all directions because the CSI of eavesdropper is unknown. Multiple antennas are used to enhance the secure communications by beamforming the information signal towards the legitimate destinations and protect it from eavesdropping or attacking. Relays play a great role in improving the physical layer security by cooperating with each other to strengthen the information rate at legitimate receiver and weaken the information rate at unauthorized users by operating as virtual multiple antennas.

Our aim in this thesis is to handle the physical layer security in TWRS and in OWRS when each node in the system has a single antenna and are working under half duplex constraint. When the global CSI is available, these systems are studied in terms of maximizing the secrecy capacity subject to the total or individual power constraint and minimizing the total power with satisfying the required QoS constraints. When CSI of the eavesdropper is not available, the available power at the relays is divided into two parts: one part is devoted to amplify and forward the information signals and the remain of the power is devoted to generate an artificial noise to jam the eavesdroppers.

1.1 Background

In this section, some concepts and theoretical details are introduced regarding the work of this thesis. Cooperative communications and relaying networks, and

their schemes used to forward the information signal between the transceivers are discussed. In addition, the concept of eigenvalues and eigenvectors is presented in order to show how to maximize or minimize a quadratic problem or a Rayleigh quotients (RQ). Most of our problems are formulated as optimization problems, and hence convex optimization is important to be introduced in this section including the Lagrange duality, KKT conditions, semidefinite programming, and optimizing RQ. Finally, physical layer security in direct and relaying transmissions is introduced.

1.1.1 Cooperative Communications

In this section, we present the principle of cooperation in communication systems, especially in wireless communications. Channels in wireless networks experience fading; meaning that there is a significant variation in the signal attenuation when it is transmitted over a wireless channel. One common solution to mitigate fading is to enable the receiver to receive multiple realizations of the transmitted signal. This technique is called diversity which can take different forms such as space diversity, time diversity, and frequency diversity. Due to the limited resources of user devices; e.g., power, complexity and size, cooperative communications have emerged to overcome these limitations since network nodes equipped with a single antenna can work together to creat a virtual antenna beam, targeting the MIMO advantages. In other words, relay nodes can work together to create a communication link between transceivers to strengthen the information signal at

the destination. In a cooperative environment, each user may act as a transceiver or as a relay that first receives the transmitted signal and then retransmits it to the destination. There are several relaying schemes that can be used in relaying systems such as

Amplify and forward (AF)

In this scheme, relays just weight the received signal by an amplification factor, then forward it to the receiver without any detection. The amplification or weight factor can be chosen to beamform the information signal to some direction.

Decode and Forward (DF)

In DF, firstly, each relay demodulates and decodes the received signal, then re-encodes the information signal, using the same or another code, and retransmits it to the receiver. DF relaying is an obstacle for physical layer security when the relay cannot be considered as a trusted node. Its ability to decode the information signal makes it easy to overhear the information signal. Therefore, some other techniques such as jamming should be applied to prevent the opportunity of eavesdropping.

Compress and forward (CF)

In CF, relays quantize the received signal and forward it to the receiver. Because compression is required, it needs more computation than AF, and at the receiver end, additional information may be required to uncompress the received message.

Among different relaying schemes, the AF scheme is the simplest one as

it does not intend to detect the received signal and it does not require any computations at relays or destination [15]. As a result, AF is adopted in this thesis for all the proposed systems.

There are two types of relaying system that are constrained to be half duplex; OWRSs and TWRSs. Fig. 1.1 shows a OWRS where there are only one transmitter, one destination, and one or multiple relays. In the first time slot, the transmitter broadcasts the message towards relays, then the relays amplify or decode the received signal (based on the relays' scheme) and forward it for the destination. In two-way relaying systems, which is shown in Fig. 1.2, the system comprises of two transceivers and one or several relays. In the first time slot, both transceivers transmit their signals towards the cooperative relays, while at the second time slot the relays amplify the signal or decode it (based on the relays' scheme) and forward it to the transceivers.

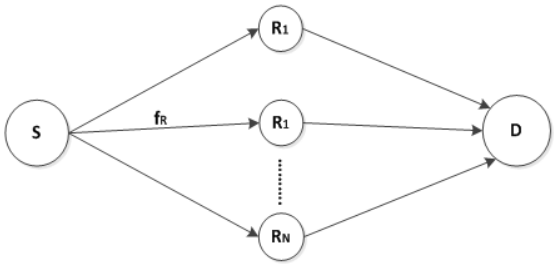

Figure 1.1: OWRS

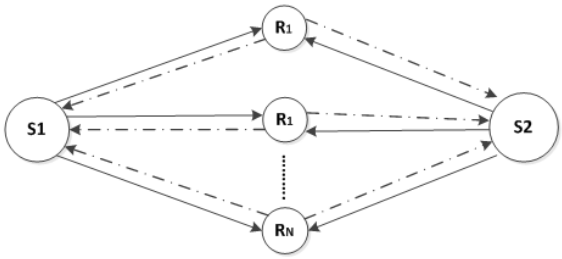

Figure 1.2: TWRS

1.1.2 Eigenvalue and Eigenvector

In this part, we will introduce the fundamentals of the eigenvalue and eigenvector. Any symmetric or Hermitian matrix A can be decomposed as

$$\mathbf{A} = U^H DU, \tag{1.1}$$

where $\mathbf{U}$ is an orthonormal matrix whose columns are the eigenvectors of $\mathbf{A}$, and $\mathbf{D}$ is a diagonal matrix whose elements are the eigenvalues of $\mathbf{A}$. If the matrix $\mathbf{A}$ is Hermitian or symmetric, the eigenvalues $\lambda_1(\mathbf{A}), \lambda_2(\mathbf{A}), ..., \lambda_n(\mathbf{A})$ are real. The eigenvalues can be obtained by solving the characteristic polynomial $det(\mathbf{A} - \lambda\mathbf{I}) = 0$. If $\mathbf{A}$ is square (i.e., number of columns equal to number of rows), we can find the the eigenvalue and eigenvector of $\mathbf{A}^2$ as

$$\mathbf{A}^2 v = \lambda \mathbf{A}\mathbf{v} = \lambda^2 \mathbf{v}.$$

Generally, for the matrix $\mathbf{A}^k$, the eigenvalue will be λ^k while the eigenvector will not change. The trace and determinant of the matrix $\mathbf{A}$ can be expressed using

eigenvalues as follows:

$$det(\mathbf{A}) = \prod_{i=1}^{n}(\lambda_i),$$

$$trace(\mathbf{A}) = \sum_{i=1}^{n}(\lambda_i).$$

The matrix $\mathbf{A}$ is called positive definite if for all nonzero vector $\mathbf{w}$, $\mathbf{w}^H\mathbf{A}\mathbf{w} > 0$. In other words, all the eigenvalues of the matrix $\mathbf{A}$ are positive. On the other hand, if all the eigenvalues of the matrix $\mathbf{A}$ are negative, $\mathbf{A}$ is called a negative definite. Also, if $\lambda_{min}(\mathbf{A}) = 0$, $\mathbf{A}$ is called positive semidefinte matrix. Similarly, $\mathbf{A}$ is called negative semidefinite matrix if $\lambda_{max}(\mathbf{A}) = 0$. If the matrix $\mathbf{A}$ has positive and negative eigenvalues, $\mathbf{A}$ is called an indefinite matrix. In this context, we denote a positive semidefinite matrix by $\mathbf{A} \succcurlyeq 0$, a positive definite matrix by $A \succ 0$ and we use $\mathbf{A} \succcurlyeq \mathbf{B}$ to denote that $\mathbf{A} - \mathbf{B} \succcurlyeq 0$. We are also interested in the generalized eigenvalues and generalized eigenvectors. The generalized eigenvalues obtained by solving the equation $det(\mathbf{x}\mathbf{B} - \mathbf{A}) = 0$, where $B \succ 0$. In other word, the generalized eigenvalues is the eigenvalues of the matrix $(\mathbf{B}^{-1}\mathbf{A})$.

1.1.3 Convex optimization

Any optimization problem, in general, can be written as minimizing an objective function subject to a group of constraints. The regular form of an optimization

problem is

$$\min_{\mathbf{x}} \quad f_0(\mathbf{x}) \tag{1.2a}$$

$$s.t \quad f_i(\mathbf{x}) \leq 0, \quad i = 1, 2, ., n \tag{1.2b}$$

$$h_j(\mathbf{x}) = 0 \quad j = 1, 2, ., m \tag{1.2c}$$

where $\mathbf{x}$ is the vector of optimization variables which can also be formed as a scalar, a vector or a matrix, f_0 is the cost function, $f_i, i = 1, .., n$, represent the inequality constraint functions, and $h_j, j = 1, ., m$,represent the equality constraint functions. If there is $\mathbf{x}$ that achieves all the constraints, we can define the problem as feasible; if not, it is infeasible. The vector that minimizes the objective function among all vectors and achieves all constraints is called the optimal solution of Problem (1.2) and we denote it by $\mathbf{x}^*$. Problem (1.2) is considered to be a linear programming if the objective and the constraint functions are affine. Any function is called affine or linear if it satisfies the following condition:

$$f(\alpha x_1 + \beta x_2) = \alpha f(x_1) + \beta f(x_2) \tag{1.3}$$

for all $x_1, x_2 \in R^n$ and $\alpha, \beta \in R$. On the other hand, Problem (1.2) can be classified as a convex problem if the cost and constraint functions are all convex [27]. The function f is called convex if it satisfies

$$f(\phi x_1 + (1 - \phi)x_2) \leq \phi f(x_1) + (1 - \phi) f(x_2), \tag{1.4}$$

where $0 \leq \phi \leq 1$. Similarly, the function f is called concave if it satisfies

$$f(\phi x_1 + (1-\phi)x_2) \geq \phi f(x_1) + (1-\phi)f(x_2), \tag{1.5}$$

where $0 \leq \phi \leq 1$. It can be seen from (1.3) and (1.4) that any linear optimization problem is convex while a convex problem is not necessarily linear. Therefore, convexity is more general then linearity [27]. There is also another way to check the problem if it is convex or not by checking the first and the second order conditions. To check the first order condition, under the assumption that the function f is differentiable, the function f is considered as a convex if and only if its domain is convex and $f(w) \geq f(v) + \nabla f(v)^T(w-v)$, for all $v, w \in dom(f)$. The second order condition states that under the assumption that f is double differentiable, that is, $\nabla^2 f$ exists at every point in its domain, which is open. Therefore, f is considered convex if and only if its domain is convex and $\nabla^2 f \succeq 0$: for all $x \in dom(f)$. The first step to solve any optimization problem is to prove whether it is convex or not. Knowing the convexity of the problem can make optimization in some sense simpler than the general case. Convexity means that it contains only one minimum value which is considered as a global minimum. When a problem is shown to be convex or can be reformulated into a convex problem, it can be directly solved by the well known tools, such as SEDUMI [2] or CVX [3].

Lagrange dual function

Considering the optimization problem (1.2) as the primary problem, the dual problem can be formulated from the primary problem by adding the cost function with the summation of weighted constraint functions. Generally, the Lagrangian dual function of Problem (1.2) is given by

$$\Gamma(x, \lambda, v) = f_0(x) + \sum_{i=1}^{m} \lambda_i f_i(x) + \sum_{i=1}^{n} v_i f_i(x) \tag{1.6}$$

Where λ_i and v_i are the Lagrange multiplier associated with the i^{th} inequality and i^{th} equality constraints, respectively. The dual function can be expressed as:

$$g(\lambda, v) = \inf_{x \in D} (f_0(x) + \sum_{i=1}^{m} \lambda_i f_i(x) + \sum_{i=1}^{n} v_i h_i(x)). \tag{1.7}$$

Assuming that P^* is the optimal solution of the primal problem (1.2) and q^* is the optimal solution of the dual problem (1.7), the following relation always is true with $\lambda \geq 0$,

$$q^* \leq p^*.$$

Generally, the solution of the dual problem and that of the primary problem would not be the same. Therefore, the Lagrange dual problem must be formulated to provide the tightest lower bound that can be attained from the dual function

which is

$$\max_{\lambda,v} \quad g(\lambda, v) \tag{1.8a}$$

$$s.t \quad \lambda \geq 0. \tag{1.8b}$$

Here, we introduce the Slater's condition which states that the objective functions of the primal and dual problems will be equal (i.e., strong duality holds), if there exists a feasible point x at which the inequality constraints hold with strict inequalities and the primal optimization problem is convex.

Karush-Kuhn-Tucker (KKT) optimality conditions

Assuming that the objective and constraint functions of an optimization problem are differentiable and satisfy Slater's condition, any pair of primal and dual optimal points have to achieve the KKT conditions. When the orignal problem is convex, the KKT conditions are sufficient for the primal and dual variables to be optimal. If x^*, λ^*, v^* are any points that satisfy the following KKT conditions:

$$f_i(\mathbf{x}^*) \leq 0 \quad i = 1, ., m \tag{1.9a}$$

$$h_i(\mathbf{x}^*) = 0, \quad i = 1, p \tag{1.9b}$$

$$\lambda_i^* \geq 0, \quad i = 1, ., m \tag{1.9c}$$

$$\lambda_i^* f_i(\mathbf{x}^*) = 0, \quad i = 1, .., m \tag{1.9d}$$

$$f_0(\mathbf{x}^*) + \sum \lambda_i^* \nabla f_i(\mathbf{x}^*) + \sum v_i^* \nabla h_i(\mathbf{x}^*) = 0 \tag{1.9e}$$

Then $\mathbf{x}$ and (λ, v) are the primal and dual optimal points with zero duality gap.

SDP

In our work, we will use a category of the convex optimization problems that is known as semidefinite programming. SDP is to minimize or maximize an affine objective function over a constraint that contains symmetric or Hermitian positive semidefinite matrices [39]. This constraint is convex but nonlinear and not smooth. Therefore, semidefinite programming problems are considered to be convex optimization problems [39]. Semidefinite programming is not much more difficult than linear programming even though they are much more general. The appropriate approach to solve the SDPs is the interior-point method. In general, we can express a semidefinite program as

$$\min_{\mathbf{X}} \quad tr(\mathbf{X}\mathbf{A}_0) \tag{1.10a}$$

$$s.t \quad tr(\mathbf{X}\mathbf{A}_i) = b_i, \quad i = 1, , m \tag{1.10b}$$

$$\mathbf{X} \succcurlyeq 0 \tag{1.10c}$$

This is called the primal expression of SDP. The dual optimization problem of SDP can be written as follows:

$$\min_{\mathbf{y}} \quad \mathbf{b}^T\mathbf{y} \tag{1.11a}$$

$$s.t \quad \mathbf{F}(\mathbf{y}) \succeq 0 \tag{1.11b}$$

where $\mathbf{F}(\mathbf{y}) = \mathbf{F}_0 + \sum_{i=1}^{m}(y_i\mathbf{F}_i), \mathbf{F}_0, \mathbf{F}_1, ., \mathbf{F}_m$ are Hermitian matrices.

Optimizing Rayleigh quotient

The generalized Rayleigh quotient (RQ) is defined as follows

$$F(x) = \frac{\mathbf{x}^H\mathbf{A}\mathbf{x}}{\mathbf{x}^H\mathbf{B}\mathbf{x}}, \tag{1.12}$$

where $\mathbf{A}$ is a symmetric matrix and $\mathbf{B} \succ 0$. The solution vector of maximizing the function $\mathbf{F}(\mathbf{x})$ is $\mathbf{x}^* = v_{max}(\mathbf{B}^{-1}\mathbf{A})$ and the solution vector of minimizing the function F(x) is $\mathbf{x}^* = v_{min}(\mathbf{B}^{-1}\mathbf{A})$.

1.1.4 Physical layer security

In this section, we introduce various physical layer security systems and the measurement metrics used to evaluate them. The simplest system investigated with physical layer security is that comprising of three terminals; source, legitimate receiver and eavesdropper. This system is shown in Fig. 1.3, in which the source desires to transmit a private message to the destination while the eavesdropper attempts to get a version of the transmitted message. The secrecy capacity of the system illustrated in Fig. 1.3 is provided in [3] as follows:

$$SC = C_D - C_E,$$

where C_D is the Shannon capacity of the destination channel and C_E is the Shannon capacity of the eavesdropper channel.

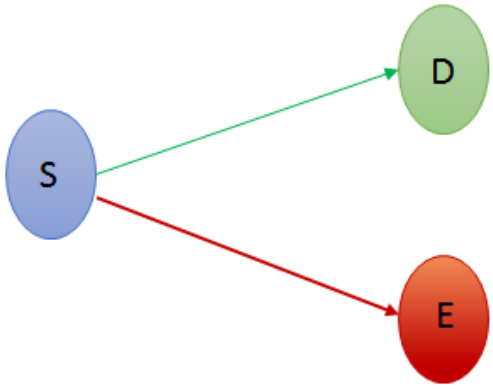

Figure 1.3: The simplest physical layer security system

It can be seen that a positive secrecy capacity can be attained if the authorized user channel is an upgraded version of the eavesdropper channel. The representation of the secrecy capacity is generalized in [4] to cover the case that the eavesdropper channel is a non-degraded form of the intended receiver. Therefore, the secrecy capacity is

$$SC = I(x_s; y_D) - I(x_s; y_E)$$

where y_D is the received signal at the destination, y_E is the received signal at eavesdropper, respectively, x_s is the transmitted symbol and $I(.;.)$ denotes the mutual information. The system illustrated in Fig. 1.3 assumes that each node has one antenna. If both source and receiver or one of them have more than one antenna, this can improve the secrecy capacity. Multiple antennas have been exploited to intensify the physical layer security using spacial diversity. In case CSI of the eavesdropper is known, MIMO can simultaneously null the information

signal at the eavesdropper and beamform it at the intended receiver [5]. Whereas, if CSI is unavailable some antennas can be used to emit artificial noise and the others can be used to beamform the signal to maximize it at the destination [6]. The idea of artificial noise is to allocate a portion of the transmitted power to generate and send a jamming signal. This artificial noise is distributed isotropically to interfere eavesdroppers since the location of them is unknown. In addition, under the assumption that the eavesdroppers are active, the source may also exploit the eavesdroppers' CSI to beamform or direct the artificial noise toward the eavesdropper for more efficient jamming such as the so-called interference alignment and cooperative jamming. In case of multiple input single output multiple eavesdropper (MISOME), if the CSI is available, the optimal beamforming vector is the generalized eigenvector related to the maximum eigenvalue of the matrix $\mathbf{H}_e^{-1}\mathbf{h}_d^H\mathbf{h}_d$, where $\mathbf{h}_d, \mathbf{H}_e$ are main channel matrix and the wiretap channel matrix, respectively [5]. In case each node has multiple antenna (MIMOME), at high SNR, the asymptotic optimal approach is to use the generalized singular value decomposition (GSVD) of the matrix $\mathbf{H}_e^{-1}\mathbf{H}_d$, where $\mathbf{H}_d$ is the main channel matrix [7]. In general, the secrecy capacity of MIMO system can be expressed as in [6]

$$SC = max_{Q \succcurlyeq 0}(\log\det(\mathbf{I} + \mathbf{H_d}\mathbf{Q}\mathbf{H_d}) - \log\det(\mathbf{I} + \mathbf{H_e}\mathbf{Q}\mathbf{H_e})),$$

where $\mathbf{Q}$ is the input covariance matrix.

The physical layer security has also been studied in cooperative systems wherein the relays can cooperate to direct the transmitted signal to the desti-

nation and degrade it at the eavesdroppers. Relays can work as relaying elements or cooperative jammers to improve the secure communications. In OWRSs, the secrecy rate is used to measure the effectiveness of physical layer security that can be expressed as follows:

$$R_S = 0.5\log(1 + SNR_D) - 0.5\log(1 + SNR_E),$$

where SNR_D, SNR_E are the SNRs at the destination and eavesdropper, respectively. In TWRSs, another metric used to measure the performance of the secure transmission called secrecy sum rate which can be expressed as follows:

$$R_{sum} = 0.5\log(1 + SNR_1) + 0.5\log(1 + SNR_2) - 0.5\log(1 + \frac{I_{e,1} + I_{e,2}}{N}),$$

where SNR_1 and SNR_2 are the SNR at the source S_1 from S_2 and the SNR at the source S_2 from S_1, respectively, and $I_{e,1}$ and $I_{e,1}$ are the information signal powers of the messages coming form the source 1 and source 2 at the eavesdropper, respectively. Generally, the predominant techniques of secure communications in relaying systems are optimal beamforming, null space beamforming, and cooperative jamming. Usually, optimal beamforming can be attained if the CSI of the eavesdropper is available and the relays use DF technique [8], [9]. In case AF technique applied, the optimal beamforming cannot be attained easily because of the non-convexity of the problem, null space beamforming has been proposed as a suboptimal approach in which all relays cooperate to null the information

signal at eavesdropper in the second phase [8], [10], [11]. Additionally, cooperative jamming has been proposed as a common solution for secure communications in both cases if the CSI of the eavesdropper is available or unavailable.

1.2 Literature Review

Physical layer security has attracted a large research interest as an important component of future wireless technology. In this part, we present the previous work of the physical layer security in direct communications and relaying systems.

1.2.1 Direct Communications

The simplest system that has been investigated is that which comprises of three terminals: transmitter, destination, and eavesdropper. Wyner [12] started to study the most basic physical layer security by showing that better secrecy capacity can be attained in the discrete memoryless wiretap channel if the source-destination channel is an upgraded version of the source-eavesdropper channel. Wyner defined the secrecy capacity of its proposed system as the highest information rate that can be achieved at the destination while maintaining the eavesdropper totally unaware of the transmitted signals. Authors of [4] generalized Wyner's work in case the transmitter wants to transmit confidential messages to Receiver 1 and public messages to both Receiver 1 and Receiver 2 while maintaining Receiver 2 as uninformed of the private messages as possible. The work of Wyner was also extended in [13] to the Gaussian channel, while an efficient

design of the secrecy scheme with flat fading channel was designed in [14]. The achievable secrecy rate for an AWGN transmitter-receiver channel is studied by [15] when the transmitter- eavesdropper channel is Rayleigh fading with additive Gaussian noise, where the CSI is known for the transmitter and receiver. They deduce that a positive secrecy rate is attainable when artificial noise is injected to jam the eavesdropper. Using MIMO in the physical layer security has attracted many researchers and engineers to enhance the secrecy in wireless networks. Multiple antennas has been investigated in [16] when the source has a single antenna and the receiver has multiple output (SIMO) aiming to show that multiple antennas would be helpful in improving secrecy rate. The work in [5] investigated the physical layer security if the channel is multiple input single output (MISO). Authors in [5] showed that multiple antennas at the source can provide the ability of beamforming to eliminate the eavesdropper rate and maximize the rate at the destination. In [6], Authors studied the physical layer security when the transmitter has multiple antenna while receiver and eavesdroppers have only one antenna. They devoted a portion of the power as an artificial noise to confuse the eavesdropper, then they studied two optimization problems: minimizing the total power under QoS on the legitimate receiver and the eavesdroppers, and maximizing the receiver SNR under total power constraints and eavesdroppers SNR. Authors of [7] and [17] studied secure communications when the channel is MIMO. In [7], Authors showed that at high SNR, high secrecy capacity can be achieved by simultaneously diagonalizing the channel matrices using the GSVD,

and independently coding over the resulting parallel channels. When only the statistical information of the eavesdropper's channel is available, authors of [18] and [19] proposed to emit an artificial noise to jam the eavesdropper. The artificial noise is designed to be orthogonal with the legitimate destination to get only the eavesdropper suffered. If the CSI of the eavesdropper channel is incompletely known, the artificial noise can be directed to some extent to the eavesdropper [20].

1.2.2 OWRS

It is known that even if each user is equipped with one antenna, they can work together to create a distributed multiple antennas system by relaying. There are several relaying schemes that can be used such as AF, DF and CF. In [21] and [22], a relay cooperation technique is proposed with one cooperative node for one direction transmission to improve the secure communications. For more than one relay, authors of [8] investigated secure communications via cooperative relays under DF, AF and cooperative jamming (CJ) under total power constraint. In [8], the closed-form optimal solution for DF with the presence of one eavesdropper is derived. In addition, if more than one eavesdropper is present, the total signal transmitted from relays is designed to be completely eliminated at the eavesdroppers in both schemes DF, AF. Whereas, for cooperative jamming, the complete jamming signal transmitted by relays is totally eliminated at the legitimate receiver. Additionally, they studied the total power minimization under secrecy rate constraint when null space beamforming is applied. A closed form solution

for this was provided. Authors of [9] proposed iterative algorithms for secrecy rate maximization under both total power constraint and individual power constraint in the presence of multiple relays. Authors of [9] used the bisection algorithm with the feasibility problem while the objective function is not guaranteed to have only one global optimal solution. To decrease the high operational complexity such as information transfer and synchronization between multiple relays, authors in [23] tried to combine the relay selection scheme and cooperative beamforming. Particularly, with full CSI and high SNR, the authors proposed selecting two relays to cooperate to null the signal at the eavesdropper. When only the phase of information is fed back between transceivers, authors in [23] proposed a distributed phase alignment and relay selection technique that modify the transmit phase at each selected relay. Physical layer security in OWRSs was also investigated by [24] using two different techniques which are beamforming with DF relaying scheme and CJ when one or more eavesdroppers are present. In [25], the authors tried to obtain the optimal beamforming vector of the relays but the optimal solution is not guaranteed because of the semidefinite relaxation (SDR) and aiming to avoid the complexity they proposed the null space beamforming as a suboptimal solution. Authors in [26], considered a system where there is only one relay and each terminal in the system has multiple antennas. They separated the channels in the system into parallel independent channels using SVD and GSVD. SVD is applied at relays beamforming while GSVD is applied at the source to diagonalize the transmitter-relays channels. In [27], physical layer security is investigated in the

existence of one helper with multiple antennas. The mission of the helper in the system of [27] is only to jam the eavesdropper without participating in relaying the information signal between the transceivers. For OWRSs, the best choice for the jammers location is to be in the vicinity of the legitimate receiver which has been proposed by [28]. Two approaches have been proposed in [28] namely, coordinated cooperative jamming and uncoordinated cooperative jamming. Authors of [29] examined a single hop system where the destination emits an artificial noise to jam the eavesdropper. When only the channel statistical information of the eavesdropper is known, authors of [30] investigated the secure communications under DF relaying scheme. They selected the best relay to forward the message while the rest of relays are determined to confuse the eavesdropper by jamming signal. In [31], Authors adopted the null space beamforming in a multiuser peer-to-peer relay system for secrecy rate maximization by optimizing the joint source and beamforming powers subject to SNR constraints at each user. They showed that the problem is difficult to optimize, then they employed a sequential parametric convex approximation approach and proposed an algorithm to develop a solution for the nonconvex problem.

1.2.3 TWRS

All the aforementioned work focuses on the physical layer security in unidirectional transmission. In [32], authors studied the physical layer security in TWRS with one untrusted relay that may work as a helper or eavesdropper. While se-

cure communications in TWRS system has been investigated with one cooperative node and one eavesdropper in [33]. For more than one relay, the authors of [34] examined the physical layer security when each relay has more than one antenna. In [10] and [11], the secure communication in TWRS has been studied in the existence of multiple distributed relays and one eavesdropper. The secrecy sum rate has been suggested as a metric to measure the effectiveness of the system for secure communications. The beamforming vector problem of TWRS with multiple relays is formulated as a product of three RQs which makes it hard to obtain the optimal solution. A suboptimal solution has been proposed where the beamforming vector was designed so as to cancel the information signals at the eavesdropper in the second phase. However, the information signals cannot be eliminated perfectly at eavesdropper since it can receive a version of the signal directly from the transmitters in the first phase. The purpose of this suboptimal solution is to reduce the optimization problem of the beamforming vector to a product of two generalized RQ. When CSI is unavailable, authors of [10] use SOCP to solve the optimization problem that minimize the information signal power under QoS constraints to reserve high power for the artificial noise. Authors of [11] also studied the problem of the total power minimization under individual secrecy rates when the null space beamforming is applied, where SDP and sequential quadratic programming are applied to find the optimal beamforming vector. In [35], the authors proposed a combination of cooperative beamforming and jamming to improve the secure communication in both transmission phases with individual power constraint. Also,

in the case of full CSI of the eavesdropper is not available, the problem can be converted to SDP with a rank one constraint. Instead of semidefinite relaxation (SDR) and randomization techniques, authors of [35] used a penalty function approach and proposed an iterative algorithm to find the weight vector of relays. Secure transmission techniques are examined in [36] for a multi-antenna bidirectional system with network coding when eavesdroppers exist. For the reason that the eavesdropper can obtain two versions of the transmitted signal, the nodes in [36] jam the eavesdropper during both phases. In [37], authors selected two or three relay nods to cooperate to jam the eavesdropper efficiently in TWRS. Authors of [38] maximized the secrecy sum rate for TWRS when the CSI is not fully available and each relay possesses only a single antenna.

1.3 Thesis Motivation

In this thesis, we study the secure communication in OWRS and TWRS. Generally, our objectives are to improve the secure communications in OWRS and TWRS, and to minimize the required power with achieving a predefined secrecy rate. Here, we outline our motivation and objectives in OWRS and TWRS.

1.3.1 OWRS

The power of relays minimization under information rates constraints

As mentioned in the literature review, Authors of [8] investigated the problem of the total power minimization under secrecy rate constraint in case the null space

beamforming is applied. This stimulates us to generalize the problem and study it when the eavesdropper information rate is not allowed to exceed some threshold. Therefore, the problem is formulated as the power of relays minimization under information rate constraints (destination and eavesdropper) when the source power is individually constrained. The problem can be expressed as follows:

$$\min_{\mathbf{w},P_s} \quad \mathbf{w}^H\mathbf{B}_0(P_s)\mathbf{w} \tag{1.13a}$$

$$s.t. \quad \mathbf{w}^H\mathbf{B}_1(P_s)\mathbf{w} \geq 1 \tag{1.13b}$$

$$\mathbf{w}^H\mathbf{B}_2(P_s)\mathbf{w} \leq 1, \tag{1.13c}$$

$$P_s \leq P_1 \tag{1.13d}$$

where P_s is the source power, P_1 is the maximum available source power, $\mathbf{w} \in C^N$, $\mathbf{w}$ is the beamforming vector at relays, $\mathbf{B}_0(P_s) \in C^{N\times N}$ is a Hermitian positive definite matrix and a function of P_s, and $\mathbf{B}_1(P_s)$, and $\mathbf{B}_2(P_s) \in C^{N\times N}$ are indefinite Hermitian matrices and functions of P_s. For the beamforming vector, although the Problem (1.13) is considered to be a QCQP which is NP-hard problem [39], it can be solved by converting it to a SDP or SOCP. Despite the complexity of SDP is in order of $O((M+N)^7)$, where N is the dimension of the column or the row in $\mathbf{B}_0$ (number of relays), and M is the number of the trace constraints, it is shown in [40] that SOCP suffers from higher complexity than the SDP approach. Motivated by this, we introduce a novel approach to solve Problem (1.13) with significantly less complexity. In addition, proposing an efficient solution for

Problem (1.13) that can be used for all (QCQPs) with positive definite objective function and two constraints.

Secrecy rate maximization under total power constraint

Although the secure communications in OWRS has been studied extensively, the optimal solution of the achievable secrecy rate maximization under total power constraint has not been achieved yet. The optimization problem is a product of two RQ which is considered as a hard problem [10], [8]. That was the motivation to develop an efficient method to obtain the optimal beamforming vector and show how much it can improve the secure communications.

1.3.2 TWRS

If the global CSI is known

From the above literature, it can be seen that the optimal weight vector and the power of sources that maximize the achievable secrecy sum rate with total power constraint are difficult to obtain. For the beamforming vector, the problem can be formulated in general as follows:

$$\max_{\mathbf{w}} \quad \frac{\mathbf{w}^H\mathbf{A}_1\mathbf{w}}{\mathbf{w}^H\mathbf{A}_2\mathbf{w}}.\frac{\mathbf{w}^H\mathbf{A}_3\mathbf{w}}{\mathbf{w}^H\mathbf{A}_4\mathbf{w}}.\frac{\mathbf{w}^H\mathbf{A}_5\mathbf{w}}{\mathbf{w}^H\mathbf{A}_6\mathbf{w}}. \tag{1.14a}$$

where $\mathbf{w} \in C^N$, $\mathbf{w}$ is the beamforming vector, and N is the number of relays, $\mathbf{A}_1, \mathbf{A}_3$ and $\mathbf{A}_6 \in C^{N\times N}$ are positive semidefinite Hermitian matrices, while $\mathbf{A}_2, \mathbf{A}_4$

and $\mathbf{A}_5 \in C^{N\times N}$ are diagonal positive definite Hermitian matrices that change according to the channels between the different nodes in the system. Problem (1.14) is neither concave nor convex which makes it difficult to solve. In [10], [11] and [35] a suboptimal approaches is adopted which is called null space beamforming to solve problem (1.14). The idea in null space beamforming is to design the weight vector $\mathbf{w}$ to be in the null space of the eavesdropper channel vector for completely eliminating the eavesdropper information rate attained in the second phase. This suboptimal approach reduces the original problem into a product of two RQs which can be written as:

$$\max_{\bar{\mathbf{q}}} \quad \frac{\bar{\mathbf{q}}^H \bar{\mathbf{A}}_1 \bar{\mathbf{q}}}{\bar{\mathbf{q}}^H \bar{\mathbf{A}}_2 \bar{\mathbf{q}}} . \frac{\bar{\mathbf{q}}^H \bar{\mathbf{A}}_3 \bar{\mathbf{q}}}{\bar{\mathbf{q}}^H \bar{\mathbf{A}}_4 \bar{\mathbf{q}}} \tag{1.15a}$$

$$s.t \quad \|\bar{\mathbf{q}}\|^2 = 1, \tag{1.15b}$$

where $\bar{\mathbf{q}} \in C^{N-2}$, and $\bar{\mathbf{A}}_1$ and $\bar{\mathbf{A}}_3 \in C^{N\times N}$ are positive semidefinite Hermitian matrices, while $\bar{\mathbf{A}}_2$ and $\bar{\mathbf{A}}_4 \in C^{N\times N}$ are a diagonal positive definite Hermitian matrices. Problem (1.15) is also hard to tackle which compel the aforementioned literature to propose suboptimal solutions for the problem (1.15). The advantage of the null space beamforming is that as the number of relays increases (goes to infinity), the optimal null space beamforming approach (the available in the literature is a suboptimal solution) rapidly approaches the optimal solution of Problem (1.14). On the other hand, the disadvantage of the null space beamforming approach is that it is inefficient when the number of relays is small since the weight vector needs to be orthogonal with two vectors which means that the available

dimensions to beamform the information signal towards sources are only $N-2$ dimensions. Besides, it is not applicable when the number of relays $N<3$. Motivated by what is mentioned above, the problem is tackled using two approaches:

1) We will propose a suboptimal solution for problem (1.14) that is efficient when the number of relays is low.

2) In case the null space beamforming is applied, we will obtain the optimal weight beamforming vector. In other words, we will find the optimal solution of the problem (1.15).

If the CSI of eavesdropper is unknown

In this case, we will investigate the artificial noise proposed in [10] for the beamforming vector to jam the eavesdropper. The problem was expressed as minimizing the information transmission power under QoS to reserve the remain of the power for the artificial noise. The problem can be expressed as follows:

$$\min_{\mathbf{w}} \quad \mathbf{w}^H \mathbf{G}_0 \mathbf{w} \tag{1.16a}$$

$$s.t. \quad \mathbf{w}^H \mathbf{G}_1 \mathbf{w} \geq \mathbf{1} \tag{1.16b}$$

$$\mathbf{w}^H \mathbf{G}_2 \mathbf{w} \geq \mathbf{1}, \tag{1.16c}$$

where $\mathbf{G}_0 \in C^{N\times N}$ is a Hermitian positive definite matrix, and $\mathbf{G}_1$, and $\mathbf{G}_2 \in C^{N\times N}$ are indefinite Hermitian matrices. In order to avoid the SDP complexity, we develop our novel approach that used to solve Problem (1.13) to tackle Problem

(1.16).

1.4 Organization and Contribution

The rest of the thesis is organized as follows:

In Chapter 2, we consider a OWRS which consists of one source, one destination, multiple cooperative relays and one eavesdropper using AF scheme. The total power of relays is minimized under information rate constraints (destination and eavesdropper) when the power of the transmitter is individually constrained. This problem is equivalent to minimizing the cost of forwarding the information signal when the relays do not forward the signal for free, which stimulate the source-destination pair to minimize the relays power where the source has a limited power. When the source power is given, the problem is formulated as a nonconvex QCQP. The optimal solution is guaranteed by reformulating the problem as a SDP that uses interior point method. Instead using SDP that suffers from high complexity, we propose a novel approach using generalized eigenvalue that provides a closed form solution in most cases. Then we prove that as the source power increases, the relays power will decrease provided that the eavesdropper constraint is satisfied.

In Chapter 3, we investigate the system adopted in Chapter 2 where the problem of maximizing the secrecy rate by looking for the optimal weight vector of the relays is solved. We show that the optimization problem is hard to tackle. Then, we convert the problem from N-dimensional search to one dimensional search with

implementing SDP problem, where N is the number of relays. Then we significantly simplify the problem by solving it using a series of eigenvalue problems and providing an efficient algorithm. Briefly, we provide the optimal beamforming vector that has not been provided yet. Compared to the null space beamforming, we prove that the optimal beamforming vector just provides a slight improvement for the secure communication especially in a high number of relays.

In Chapter 4, we study the secure communications in a TWRS comprising of two transceivers, one eavesdropper, and several relays. The system is studied in case the CSI of the eavesdropper is available. The problem of maximizing the secrecy sum rate is adopted under total power constraint. For the beamforming vector, until now, suboptimal solutions have been proposed for the null space beamforming in the literature. Accordingly, in Chapter 4, we propose two approaches: 1) the optimal null space beamforming approach, 2) Ignoring one RQ. In the first approach, for beamforming vector, we convert the nonconvex product of two RQs to a convex problem with one dimensional search using semidefinite programming (SDP). Then we significantly simplify the problem using the generalized eigenvalues. While for sources power, we solve the problem using Newton algorithm. In the second approach, we deal with beamforming vector that does not cancel the information signal at the eavesdropper aiming to increase the whole secrecy sum rate. Therefore, we ignore one Rayleigh quotient out of three that has less impact on the whole function and optimize the problem.

In Chapter 5, we investigate the secure communications in the same system

studied in Chapter 4 in case the CSI of the eavesdropper is unobtainable, and hence artificial noise is applied to impair the information signal at the eavesdropper. In order to reserve the maximum possible power for artificial noise, the problem of minimizing the total power of the information signal transmitted by the relays under QoS constraints at the transceivers is considered. This problem has been solved using SDP and SOCP methods. Here, aiming to significantly decrease the complexity, we propose a novel approach to obtain the optimal solution using the generalized eigenvalue. We show that in most cases, we can provide a closed-form expression of the optimal solution. In addition, our proposed solution can be used for all quadratically constrained quadratic programs (QCQPs) with positive definite objective function and two constraints. Simulation results demonstrate the effectiveness of our algorithm in terms of optimality and low complexity compared to SDP.

In Chapter 6, we conclude the thesis by highlighting the core contributions and conclusions achieved in this work. Moreover, some future work in the physical layer security in relay system is proposed.

CHAPTER 2

RELAYS TOTAL POWER MINIMIZATION UNDER SECRECY CONSTRAINT IN OWRS

In this chapter, we consider a OWRS which consists of one transmitter, one receiver, multiple cooperative relays and one eavesdropper using amplify and forward (AF) scheme. Each node in the system has only one antenna, and is working under half duplex constraint. We minimize the power of relays under information rate constraints for both the legitimate destination and the eavesdropper when the source power is individually constrained. This problem is required to be studied when the source-destination pair must pay to the relays for forwarding the transmitted signal, which stimulates the source-destination pair to minimize the

power of relays when the source has a limited power. When the source power is given, the problem is formulated as a non-convex QCQP. The optimal solution is guaranteed by reformulating the problem as SDP that uses interior point method. Instead of using SDP that suffers from high complexity, we propose a novel approach using generalized eigenvalue that provides a closed form solution in most cases. Then we prove that as the source power increases, the relays' total power will decrease as long as the eavesdropper constraint is feasible. Simulation results demonstrate that the proposed approach achieves the optimal solution of the relay beamforming vector with significant lower complexity.

The rest of this chapter is organized as follows, the system model is introduced in Section 2.2. In Section 2.3, we present the achievable secrecy rate. Section 2.4 is devoted for the problem formulation and proposed solution. numerical results is showed in Section 2.5 and we present the conclusion in Section 2.6.

2.1 System Model

We propose a OWRS that comprises a source S, a destination D, an eavesdropper E, and N trusted relay nodes. Each node in the system has only single antenna, and is working under a half duplex constraint. The system is investigated according to the assumption that the global CSI of the eavesdropper is available. This CSI can be attained if the eavesdropper is active and its transmission can be observed. It is assumed that a direct connection between the transmitter and both the eavesdropper and legitimate receiver is not available. The codewords at

the source are assumed to be Gaussian. We assume that each channel is a block fading channel that changes from one block to another according to a Rayleigh distribution. We denote by $\mathbf{f}_R$ the complex transmitter-relay nodes channel gain vector $(N \times 1)$, by $\mathbf{g}_d$ the relays-destination channel vector $(N \times 1)$, and by $\mathbf{g}_e$ the complex relays-eavesdropper channel gain vector. In amplify and forward scheme,

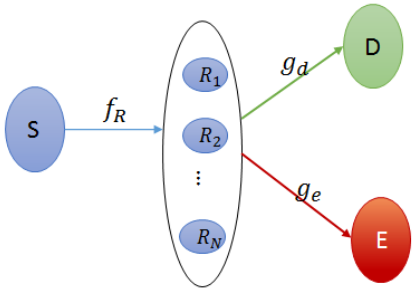

Figure 2.1: System model

the signal is transmitted over two time slots. In the first one the transmitter broadcasts the signal to the cooperative relays. The received signal at the relays can be written as:

$$\mathbf{y}_R = \sqrt{P_s}\mathbf{f}_R x + \mathbf{n}_R, \tag{2.1}$$

where P_s is the power of the transmitter, x is the symbol transmitted by the source with unit power, and $\mathbf{n}_R$ is the complex Gaussian noise vector at the relays with zero mean and variance $\sigma_R^2\mathbf{I}_n$. In the second phase, each trusted relay weights the noisy received signal, then retransmits it to the receiver. Therefore, the transmitted signal of all relays can be expressed as $diag(\mathbf{w})\mathbf{y}_R$, where $\mathbf{y}_R$ is given by (2.1), and $\mathbf{w}$ is the complex beamforming vector that weights the received

signal at the relays. Therefore, the received signal at the destination attained from the second phase can be expressed as:

$$y_D^{(2)} = \sqrt{P_s}\mathbf{w}^H\mathbf{a}_{fd}x + \mathbf{w}^H\mathbf{G}_d\mathbf{n}_R + n_D, \tag{2.2}$$

where $\mathbf{G}_d = diag(\mathbf{g}_d)$, $\mathbf{a}_{fd} = \mathbf{G}_d^H\mathbf{f}_R$ and n_D is the additive zero mean noise with σ_D^2 at destination. The eavesdropper can receive a version of the information signal which can be written as:

$$y_E = \sqrt{P_s}\mathbf{w}^H\mathbf{a}_{fe}x + \mathbf{w}^H\mathbf{G}_e\mathbf{n}_R + n_E, \tag{2.3}$$

where $\mathbf{G}_e = diag(\mathbf{g}_e), \mathbf{a}_{fe} = \mathbf{G}_e^H\mathbf{f}_R$, and n_E is the additive zero mean noise with variance σ_E^2 at the eavesdropper.

2.2 Achievable Secrecy Rate

In this section, we formulate the information rate received at the intended receiver, the information rate received at the eavesdropper, and the secrecy rate. From (2.2), the information rate attained at the destination can be written as follows:

$$R_d = \frac{1}{2}\log(1 + \frac{P_s\mathbf{w}^H\mathbf{R}_{fd}\mathbf{w}}{\sigma_D^2 + \sigma_R^2\mathbf{w}^H\mathbf{R}_{gg}\mathbf{w}}), \tag{2.4}$$

where $\mathbf{R}_{fd} = \mathbf{a}_{fd}\mathbf{a}_{fd}^H$, $\mathbf{R}_{gg} = \mathbf{G}_d^H\mathbf{G}_d$. The scalar factor $\frac{1}{2}$ is due to that the transmitted signal consumes two time slots. Similarly the information rate attained at

the eavesdropper is

$$R_e = \frac{1}{2}\log(1 + \frac{P_s \mathbf{w}^H \mathbf{R}_{fe} \mathbf{w}}{\sigma_E^2 + \sigma_R^2 \mathbf{w}^H \mathbf{R}_{ee} \mathbf{w}}), \tag{2.5}$$

where $\mathbf{R}_{fe} = \mathbf{a}_{fe}\mathbf{a}_{fe}^H$, $\mathbf{R}_{ee} = \mathbf{G}_e^H \mathbf{G}_e$. The secrecy rate as shown in [5] , [17] and [8] can be expressed as follows:

$$R_s = \frac{1}{2}\log(1 + \frac{P_s \mathbf{w}^H \mathbf{R}_{fd} \mathbf{w}}{\sigma_D^2 + \sigma_R^2 \mathbf{w}^H \mathbf{R}_{gg} \mathbf{w}}) - \frac{1}{2}\log(1 + \frac{P_s \mathbf{w}^H \mathbf{R}_{fe} \mathbf{w}}{\sigma_E^2 + \sigma_R^2 \mathbf{w}^H \mathbf{R}_{ee} \mathbf{w}}). \tag{2.6}$$

The relays' transmit power can be obtained by

$$P_r = E\{(diag(\mathbf{w})\mathbf{y}_R)^H (diag(\mathbf{w})\mathbf{y}_R)\} = \mathbf{w}^H \mathbf{T} \mathbf{w},$$

where $\mathbf{T}$ is a diagonal matrix $\mathbf{T} = P_s \mathbf{F} + \sigma^2 \mathbf{I}_N$, where $\mathbf{F} = diag(\mathbf{f}_R^H) diag(\mathbf{f}_R)$.

2.3 Power of Relays Minimization

In this section, we minimize the power of relays under a given information rate constraints in the legitimate destination and the eavesdropper when the source power is individually constrained. We intend to find the optimal beamforming vector $\mathbf{w}$ and the source power P_s that minimize the relays' total power and

achieve the given information rates. The problem can be written as follows:

$$\min_{\mathbf{w},P_s} \quad \mathbf{w}^H(P_s\mathbf{R}_{ff}+\sigma^2\mathbf{I}_N)\mathbf{w} \tag{2.7a}$$

$$s.t \quad 0.5\log(1+\frac{P_s\mathbf{w}^H\mathbf{R}_{fd}\mathbf{w}}{\sigma_D^2+\sigma_R^2\mathbf{w}^H\mathbf{R}_{gg}\mathbf{w}})\geq r_d, \tag{2.7b}$$

$$0.5\log(1+\frac{P_s\mathbf{w}^H\mathbf{R}_{fe}\mathbf{w}}{\sigma_E^2+\sigma_R^2\mathbf{w}^H\mathbf{R}_{ee}\mathbf{w}})\leq r_e, \tag{2.7c}$$

$$P_s\leq P_1, \tag{2.7d}$$

where r_d and r_e are the minimum required information rate at the destination and the maximum allowable eavesdropper's information rate, respectively, and P_1 is the maximum available source power. Problem (2.7) is not convex, and hence it is difficult to solve for the global optimal. Therefore, we obtain the optimal beamforming vector when the source power is fixed, then we propose an algorithm that guarantees the joint global optimal solution $(P_s^*,\mathbf{w}^*)$.

2.3.1 Beamforming Vector Optimization

Here, we solve Problem (2.7) when the source power P_s is fixed. Therefore, the problem is equivalent to minimize the relays transmit power under information rate constraints. Define $\delta\in[0,1]$, $\delta=\frac{r_e}{r_d}$; the ratio of the allowable maximum eavesdropper's information rate to the minimum destination's information rate. The problem is written as:

$$\min_{\mathbf{w}} \quad \mathbf{w}^H(P_s\mathbf{R}_{ff} + \sigma^2\mathbf{I}_N)\mathbf{w} \tag{2.8a}$$

$$s.t \quad \mathbf{w}^H(P_s\mathbf{R}_{fd} - t_d\sigma_R^2\mathbf{R}_{gg})\mathbf{w} \geq \sigma_D^2 t_d \tag{2.8b}$$

$$\mathbf{w}^H(P_s\mathbf{R}_{fe} - t_e\sigma_R^2\mathbf{R}_{cc})\mathbf{w} \leq \sigma_E^2 t_e, \tag{2.8c}$$

where $t_d = 2^{2r_d} - 1$, and $t_e = 2^{2\delta r_d} - 1$. Let $\mathbf{B}_0 = (P_s\mathbf{R}_{ff} + \sigma^2\mathbf{I}_N)$, $\mathbf{B}_1 = \frac{1}{\sigma_D^2 t_d}(P_s\mathbf{R}_{fd} - \sigma_R^2 t_d\mathbf{R}_{gg})$ and $\mathbf{B}_2 = \frac{1}{\sigma_e^2 t_e}(P_s\mathbf{R}_{fe} - \sigma_R^2 t_e\mathbf{R}_{cc})$. Therefore, we can rewrite (2.8) as:

$$\min_{\mathbf{w}} \quad \mathbf{w}^H\mathbf{B}_0\mathbf{w} \tag{2.9a}$$

$$s.t. \quad \mathbf{w}^H\mathbf{B}_1\mathbf{w} \geq \mathbf{1} \tag{2.9b}$$

$$\mathbf{w}^H\mathbf{B}_2\mathbf{w} \leq \mathbf{1}, \tag{2.9c}$$

$\mathbf{B}_0$ can be shown to be a positive definite matrix, while $\mathbf{B}_1$ and $\mathbf{B}_2$ are indefinite matrices. Problem (2.9) is a not convex QCQP problem, but it can be reformulated as a SDP with rank constraint as:

$$\min_{\mathbf{W}} \quad tr(\mathbf{W}\mathbf{B}_0) \tag{2.10a}$$

$$s.t. \quad tr(\mathbf{W}\mathbf{B}_1) \geq 1 \tag{2.10b}$$

$$tr(\mathbf{W}\mathbf{B}_2) \leq 1 \tag{2.10c}$$

$$\mathbf{W} \succeq 0, \quad Rank(\mathbf{W}) = 1. \tag{2.10d}$$

The constraint (2.10d) guarantees that the matrix $\mathbf{W}$ can be written as $\mathbf{W} = \mathbf{w}\mathbf{w}^H$. Problem (2.10) is not convex because of the rank constraint of $\mathbf{W}$. In [41], it was shown that if the number of the trace constraints is n, then the global optimal solution matrix $\mathbf{W}$ will have a rank $r \leq \sqrt{n}$. Here, in Problem (2.10), the number of trace constraints is two traces which means that the solution matrix $\mathbf{W}$ will definitely have rank one, and hence Problem (2.10) is equivalent to the following problem

$$\min_{\mathbf{W}} \quad tr(\mathbf{W}\mathbf{B}_0) \tag{2.11a}$$

$$s.t. \quad tr(\mathbf{W}\mathbf{B}_1) \geq 1 \tag{2.11b}$$

$$tr(\mathbf{W}\mathbf{B}_2) \leq 1 \tag{2.11c}$$

$$\mathbf{W} \succeq 0, \tag{2.11d}$$

where the optimal beamforming vector $\mathbf{w}$ is the eigenvector related to the non-zero eigenvalue of the optimal $\mathbf{W}$. Although, SDP can provide the optimal beamforming vector, it suffers from high complexity. Authors of [11] show that the complexity of SDP problem is $O((N+K)^7)$, where K is the number of the trace constraints and N is the row or column dimension of $\mathbf{B}_0$ (number of relays). Therefore, here we propose an alternative solution for the SDP problem that provides the optimal beamforming vector with significant decrease in complexity. First, it is direct to show that in Problem (2.11), the first inequality constraint (2.11b) achieved with equality at optimality. If not, the beamforming vector can be scaled down to enforce the constraint to be active without violating the second

constraint, which causes a diminution in the objective function. Whereas this is not applied for the second constraint.

Theorem 2.1 *If the constraint (2.11c) does not hold with equality which means that only constraint (2.11b) holds with equality, the optimal beamforming vector is* $\mathbf{w}^* = \mathbf{w}_1 = \frac{1}{\sqrt{\mathbf{v}_1^H \mathbf{B}_1 \mathbf{v}_1}} \mathbf{v}_1$ *, where* $\mathbf{v}_1 = \mathbf{v}_{max}(\mathbf{B}_0^{-1}\mathbf{B}_1)$.

Proof. The problem in (2.11) is convex given that the objective and the constraints functions are convex. In addition, Problem (2.11) satisfies Slater's condition which states that strong duality holds if there exists a feasible point at which the inequality constraints hold with strict inequalities and the primal optimization problem is convex (details in [42]). Thus, the KKT conditions are sufficient and necessary for a primal-dual point to be optimal. The Lagrangian function of problem (2.11) is

$$\Gamma = tr(\mathbf{W}\mathbf{B}_0) - tr(\mathbf{W}\mathbf{Q}) - \beta_0 tr(\mathbf{W}\mathbf{B}_1) + \beta_1 tr(\mathbf{W}\mathbf{B}_2) + \beta_0 - \beta_1, \tag{2.12}$$

where $\beta_0 \geq 0, \beta_1 \geq 0$ and $\mathbf{Q} \succeq 0$ are the Lagrangian dual variables. The KKT

conditions are:

$$\frac{d\Gamma}{d\mathbf{W}} = \mathbf{B}_0 - \mathbf{Q}^* - \beta_0^*\mathbf{B}_1 + \beta_1^*\mathbf{B}_2 = 0 \tag{2.13a}$$

$$tr(\mathbf{W}^*\mathbf{B}_1) - 1 \geq 0 \tag{2.13b}$$

$$tr(\mathbf{W}^*\mathbf{B}_2) - 1 \leq 0 \tag{2.13c}$$

$$tr(\mathbf{W}^*\mathbf{Q}^*) = 0 \tag{2.13d}$$

$$\beta_0^* tr(\mathbf{W}^*\mathbf{B}_1) - \beta_0^* = 0 \tag{2.13e}$$

$$\beta_1^* tr(\mathbf{W}^*\mathbf{B}_2) - \beta_1^* = 0 \tag{2.13f}$$

$$\mathbf{W}^* \succeq 0, \quad \mathbf{Q}^* \succeq 0 \quad \beta_0^* \geq 0 \quad \beta_1^* \geq 0. \tag{2.13g}$$

From KKT conditions, in particular (2.13a), the dual optimization problem can be written as

$$\max_{\beta_0,\beta_1} \quad \beta_0 - \beta_1 \tag{2.14a}$$

$$s.t. \quad \mathbf{B}_0 - \beta_0\mathbf{B}_1 + \beta_1\mathbf{B}_2 \succeq 0, \tag{2.14b}$$

$$\beta_0 \geq 0, \beta_1 \geq 0. \tag{2.14c}$$

Under the assumption that the constraint (2.11c) does not hold with equality, β_1^* must be zero to satisfy the KKT conditions. Therefore, problem (2.14) can be

written as:

$$\max_{\beta_0,\beta_1} \quad \beta_0 \tag{2.15a}$$

$$s.t. \quad \mathbf{B}_0 - \beta_0\mathbf{B}_1 \succeq 0, \tag{2.15b}$$

$$\beta_0 \geq 0. \tag{2.15c}$$

In fact, it can be seen that (2.11b) holds with equality while (2.11c) doesn't when $tr(\mathbf{W}^*\mathbf{B}_1) > tr(\mathbf{W}^*\mathbf{B}_2)$ and $\mathbf{w}^{*H}\mathbf{B}_1\mathbf{w}^* > \mathbf{w}^{*H}\mathbf{B}_2\mathbf{w}^*$. Furthermore, at optimality, both the objective function of the primal and dual optimization problems are equal, β_0^*=$tr(\mathbf{W}^*\mathbf{B}_0)$=$\frac{tr(\mathbf{W}^*\mathbf{B}_0)}{tr(\mathbf{W}^*\mathbf{B}_1)}$=$\frac{\mathbf{w}^{*H}\mathbf{B}_0\mathbf{w}^*}{\mathbf{w}^{*H}\mathbf{B}_1\mathbf{w}^*}$. In addition, from the constraint (2.15b) we have $\mathbf{I} \succeq \beta_0^*\mathbf{B}_0^{-1}\mathbf{B}_1$, so $\frac{1}{\beta_0^*}\mathbf{I} \succeq \mathbf{B}_0^{-1}\mathbf{B}_1$, $\frac{1}{\beta_0^*} \geq \lambda_{max}(\mathbf{B}_0^{-1}\mathbf{B}_1)$ which means that the maximum value of β_0^* is $\frac{1}{\lambda_{max}(\mathbf{B}_0^{-1}\mathbf{B}_1)}$. Hence,

$$\frac{\mathbf{w}^{*H}\mathbf{B}_1\mathbf{w}^*}{\mathbf{w}^{*H}\mathbf{B}_0\mathbf{w}^*} = \frac{1}{\beta_0^*} = \lambda_{max}(\mathbf{B}_0^{-1}\mathbf{B}_1). \tag{2.16}$$

The optimal beamforming vector that satisfies (2.16) is $\mathbf{v}_{max}(\mathbf{B}_0^{-1}\mathbf{B}_1)$ =$\mathbf{v}_1$. But we have to scale the solution vector to satisfy the constraints since the scaling does not affect on the relation (2.16). Hence, we have $\mathbf{w}^*$=$\frac{1}{\sqrt{\mathbf{v}_1^H\mathbf{B}_1\mathbf{v}_1}}\mathbf{v}_1$ aiming to have the constraint (2.11b) active while having the constraint (2.11c) strict. ∎

It is important to say that, the constraint (2.11c) might or might not hold with equality while the constraint (2.11b) always holds with equality, so we have only two cases which are: 1) the first constraint only holds with equality. 2) both constraints hold with equality. We have provided a closed form solution of the

first case while in the following we propose an algorithm that provides a solution for the second case. Obviously, Both constraints hold with equality means that $\beta_0^* > 0$ and $\beta_1^* > 0$, which means that $\frac{1}{\sqrt{\mathbf{v}_1^H \mathbf{B}_1 \mathbf{v}_1}} \mathbf{v}_1$ cannot be a solution for the problem (2.9). We propose another solution for Case 2, other than the SDP approach to avoid the complexity. The problem (2.11) can be written as:

$$\min_{\mathbf{W}} \quad tr(\mathbf{W}\mathbf{B}_0) \tag{2.17a}$$

$$s.t \quad tr(\mathbf{W}\mathbf{B}_1) = 1 \tag{2.17b}$$

$$tr(\mathbf{W}\mathbf{B}_2) = 1 \tag{2.17c}$$

$$\mathbf{W} \succeq 0, \tag{2.17d}$$

Theorem 2.2 *the optimal solution vector of Problem (2.17) is a weighted version of the optimal solution vector of the following problem*

$$\max_{\mathbf{V}} \quad tr(\mathbf{V}\mathbf{B}_1) \tag{2.18a}$$

$$s.t \quad tr(\mathbf{V}\mathbf{B}_0) \leq 1 \tag{2.18b}$$

$$tr(\mathbf{V}\mathbf{B}_1) = tr(\mathbf{V}\mathbf{B}_2) \tag{2.18c}$$

$$\mathbf{V} \succeq 0. \tag{2.18d}$$

In other words, $\mathbf{w}^* = \frac{1}{\sqrt{\mathbf{v}^{*H} \mathbf{B}_1 \mathbf{v}^*}} \mathbf{v}^*$*, where the optimal solution* $\mathbf{v}^*$ *is the solution vector of the problem in (2.18), where* $\mathbf{V} = \mathbf{v}\mathbf{v}^H$.

Proof. Assuming $\mathbf{W} = \mathbf{w}\mathbf{w}^H$, if we substitute $\mathbf{w}$ by $\frac{1}{\sqrt{\mathbf{v}^H\mathbf{B}_1\mathbf{v}}}\mathbf{v}$, we can write the problem in (2.17) as

$$\min_{\mathbf{v}} \quad \frac{\mathbf{v}^H\mathbf{B}_0\mathbf{v}}{\mathbf{v}^H\mathbf{B}_1\mathbf{v}} \tag{2.19a}$$

$$s.t. \quad \frac{\mathbf{v}^H\mathbf{B}_1\mathbf{v}}{\mathbf{v}^H\mathbf{B}_1\mathbf{v}} = 1 \tag{2.19b}$$

$$\frac{\mathbf{v}^H\mathbf{B}_2\mathbf{v}}{\mathbf{v}^H\mathbf{B}_1\mathbf{v}} = 1. \tag{2.19c}$$

The constraint (2.19b) can obviously be removed, and using the inverse of the objective function in (2.19a), the problem in (2.19) can be written as:

$$\max_{\mathbf{v}} \quad \frac{\mathbf{v}^H\mathbf{B}_1\mathbf{v}}{\mathbf{v}^H\mathbf{B}_0\mathbf{v}} \tag{2.20a}$$

$$s.t. \quad \mathbf{v}^H\mathbf{B}_2\mathbf{v} = \mathbf{v}^H\mathbf{B}_1\mathbf{v}. \tag{2.20b}$$

The expression $\mathbf{v}^H\mathbf{B}_0\mathbf{v}$ is considered as a normalizing vector that can be converted to a constraint $\mathbf{v}^H\mathbf{B}_0\mathbf{v} = \mathbf{1}$, and hence both Problems (2.20) and (2.17) are equivalent. ∎

In the following, we provide a simple and efficient algorithm to find the optimal vector $\mathbf{v}^*$, in order to avoid the complexity of the SDP approach. The dual problem of problem (2.18) can be written as

$$\min_{\alpha,\mu} \quad \alpha \tag{2.21a}$$

$$s.t. \quad -\mathbf{B}_1 + \alpha\mathbf{B}_0 - \mu(\mathbf{B}_2 - \mathbf{B}_1) \succeq 0, \tag{2.21b}$$

$$\alpha \geq 0 \tag{2.21c}$$

From (2.21b), we can write α as

$$\alpha \mathbf{I} \succeq (\mathbf{1}-\mu)\mathbf{B}_0^{-1}\mathbf{B}_1 + \mu \mathbf{B}_0^{-1}\mathbf{B}_2.$$

Therefore, the optimal value of α must satisfy that

$$\alpha^* = \min_{\mu} \lambda_{max}((\mathbf{1}-\mu)\mathbf{B}_0^{-1}\mathbf{B}_1 + \mu \mathbf{B}_0^{-1}\mathbf{B}_2).$$

Here, we raise a question: what is the relation between α^* and $\mathbf{v}^*$?. Let $\mathbf{x} = \mathbf{v}_{max}((1-\mu^*)\mathbf{B}_0^{-1}\mathbf{B}_1 + \mu^*\mathbf{B}_0^{-1}\mathbf{B}_2)$, then

$$\alpha^* = \mathbf{x}^H((1-\mu^*)\mathbf{B}_0^{-1}\mathbf{B}_1 + \mu^*\mathbf{B}_0^{-1}\mathbf{B}_2)\mathbf{x} = (1-\mu^*)\frac{\mathbf{x}^H\mathbf{B}_1\mathbf{x}}{\mathbf{x}^H\mathbf{B}_0\mathbf{x}} + \mu^*\frac{\mathbf{x}^H\mathbf{B}_2\mathbf{x}}{\mathbf{x}^H\mathbf{B}_0\mathbf{x}}.$$

From the convexity of the problem and the fact that Slater's condition is satisfied, it can be shown that strong duality holds for the Problem (2.17). Therefore, the optimal solution of the primal and dual problems are equal; i.e., $\alpha^* = \frac{\mathbf{v}^{*H}\mathbf{B}_1\mathbf{v}^*}{\mathbf{v}^{*H}\mathbf{B}_0\mathbf{v}^*}$, and μ must be selected to satisfy $\mathbf{v}^{*H}\mathbf{B}_1\mathbf{v}^* = \mathbf{v}^{*H}\mathbf{B}_2\mathbf{v}^*$. Therefore,

$$\alpha^* = \frac{\mathbf{v}^{*H}\mathbf{B}_1\mathbf{v}^*}{\mathbf{v}^{*H}\mathbf{B}_0\mathbf{v}} = (1-\mu^*)\frac{\mathbf{v}^{*H}\mathbf{B}_1\mathbf{v}^*}{\mathbf{v}^{*H}\mathbf{B}_0\mathbf{v}^*} + \mu^*\frac{\mathbf{v}^{*H}\mathbf{B}_2\mathbf{v}^*}{\mathbf{v}^{*H}\mathbf{B}_0\mathbf{v}^*} = (1-\mu^*)\frac{\mathbf{x}^H\mathbf{B}_1\mathbf{x}}{\mathbf{x}^H\mathbf{B}_0\mathbf{x}} + \mu^*\frac{\mathbf{x}^H\mathbf{B}_2\mathbf{x}}{\mathbf{x}^H\mathbf{B}_0\mathbf{x}}$$

, and hence,

$$\mathbf{v}^* = \mathbf{x} = \mathbf{v}_{max}((1-\mu^*)\mathbf{B}_0^{-1}\mathbf{B}_1 + \mu^*\mathbf{B}_0^{-1}\mathbf{B}_2). \tag{2.22}$$

In order to find $\mathbf{v}^*$, we use the bisection algorithm to find the optimal value

of μ which must yield a vector $\mathbf{v}^*$ that satisfies the equality $\mathbf{v}^{*H}\mathbf{B}_1\mathbf{v}^*=\mathbf{v}^{*H}\mathbf{B}_2\mathbf{v}^*$ with a tolerance of ϵ. Therefore, the following algorithm is used to find $\mathbf{v}^*$.

Algorithm 2.1 Find the beamforming vector for Problem (2.9) when both constraints are active.

1. Determine the maximum and minimum value of μ; i.e. define μ_{min} and μ_{max} (finding μ_{max} and μ_{min} is explained after Step 5).
2. Let $m = (\mu_{min} + \mu_{max})/2$, then find $\mathbf{v} = \mathbf{v}_{max}((1-\mu)\mathbf{B}_0^{-1}\mathbf{B}_1 + \mu\mathbf{B}_0^{-1}\mathbf{B}_2)$ with $\mu = m$.
3. If $\mathbf{v}^H\mathbf{B}_1\mathbf{v} < \mathbf{v}^H\mathbf{B}_2\mathbf{v}$, $\mu_{\max} = m$, else if $\mathbf{v}^H\mathbf{B}_1\mathbf{v} > \mathbf{v}^H\mathbf{B}_2\mathbf{v}$, $\mu_{min} = m$.
4. If $|\mathbf{v}^H\mathbf{B}_1\mathbf{v} - \mathbf{v}^H\mathbf{B}_2\mathbf{v}| \leq \varepsilon$, $\mu^* = (\mu_{min} + \mu_{\max})/2$, otherwise go back to step 2.
5. Find $\mathbf{v}^* = \mathbf{v}_{\max}((\mathbf{1} - {}^{-*})\mathbf{B}_0^{-1}\mathbf{B}_1 + \mu^*\mathbf{B}_0^{-1}\mathbf{B}_2)$ then find $\mathbf{w}^*=\frac{1}{\sqrt{\mathbf{v}^{*H}\mathbf{B}_1\mathbf{v}^*}}\mathbf{v}^*$.

μ_{min} and μ_{max} should be determined to achieve that $\mathbf{v}^H(\mu_{min})\mathbf{B}_1\mathbf{v}(\mu_{min}) < \mathbf{v}^H(\mu_{min})\mathbf{B}_2\mathbf{v}(\mu_{min})$ and $\mathbf{v}(\mu_{max})^H\mathbf{B}_1\mathbf{v}(\mu_{max}) > \mathbf{v}(\mu_{max})^H\mathbf{B}_2\mathbf{v}(\mu_{max})$; i.e, there is a cross point between μ_{min} and μ_{max} which guarantees that $\mathbf{v}^H\mathbf{B}_1\mathbf{v} = \mathbf{v}^H\mathbf{B}_2\mathbf{v}$.

Therefore, the algorithm to solve Problem (2.9) to obtain $\mathbf{w}^*$ is

Algorithm 2.2 Finding the optimal beamforming vector of Problem (2.9) when the source power is fixed.

1. find $\mathbf{w}_1=\frac{1}{\sqrt{\mathbf{v}_1^H\mathbf{B}_1\mathbf{v}_1}}\mathbf{v}_1$.
2. If $\mathbf{w}_1$ is feasible,$\mathbf{w}^* = \mathbf{w}_1$
3. If $\mathbf{w}_1$ is infeasible, use Algorithm 2.1 to have the optimal vector.

2.3.2 Source power Problem

In this section, we obtain the optimal source power that minimizes the relays' transmit power. As demonstrated before that the constraint (2.11b) must be ac-

tive (holds with equality) to minimize the relaying transmit power, and increasing P_s enforces the relays to decrease their power aiming to satisfy the same information rate at the receiver and keep the eavesdropper information rate under the given threshold. In other words, increasing the power of the source relaxes the objective function (2.8a) to some extent from the constraints (2.8b) and (2.8c). Therefore, the optimal value of the source power for the optimization problem (2.11) is it's maximum value (i.e., $P_s^* = P_1$) provided that Problem (2.11) is feasible. Otherwise, source power P_s should be decreased until Problem (2.11) be feasible.

Here, we propose an algorithm that provides the joint optimal solution ($P_s^*, \mathbf{w}^*$) which minimizes the power of relays:

Algorithm 2.3 Algorithm for finding the joint optimal solution for Problem (2.8).

---

1. Given the maximum available source power P_1, use Algorithm 2.2 to solve Problem (2.11) to obtain the beamforming vector when $P_s = P_1$.
2. If Problem (2.11) is not feasible,
3. $P_s = P_1 - \Delta P_1$,
4. else break,
5. (where ΔP_1 is a very small positive value compared to P_1).
6. Repeat step 1 and 2 until we get Problem 2.8 feasible, otherwise, P_s will reach zero which means that the information rates (r_d and r_e) cannot be achieved with the given channels.

2.4 Simulation Results

In this part, the effectiveness of the proposed algorithms are evaluated. In each simulation result, we generate all the channels randomly as independent complex Gaussian random variables with zero mean and unit variance. All SDPs are solved efficiently using interior point method provided by Matlab CVX toolbox [3]. We obtain the results by averaging over 2000 Monte Carlo channel realization. In

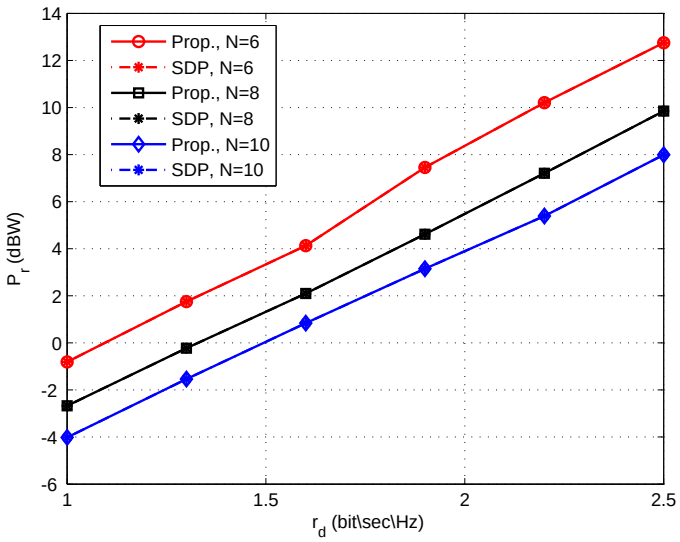

Figure 2.2: comparison of our Algorithm 2.3 that uses our proposed solution to find w and Algorithm 2.3 that uses SDP with different number of relays, $\delta = 0.1$, and $P_1 = 15\ dBW$.

Fig. 2.2, we implement Algorithm 2.3 for the power of the relays minimization by finding the joint optimal solution $(P_s^*, \mathbf{w}^*)$ versus the minimum required information rate at the destination for various number of relays when $r_e = 0.1 r_d$ and the maximum available power at the source is $P_1 = 15\ dBW$. We obtain the beamforming vector in Algorithm 2.3 (step 1) using two approaches: SDP and our proposed Algorithm 2.2, and we show that both approaches provide an identical

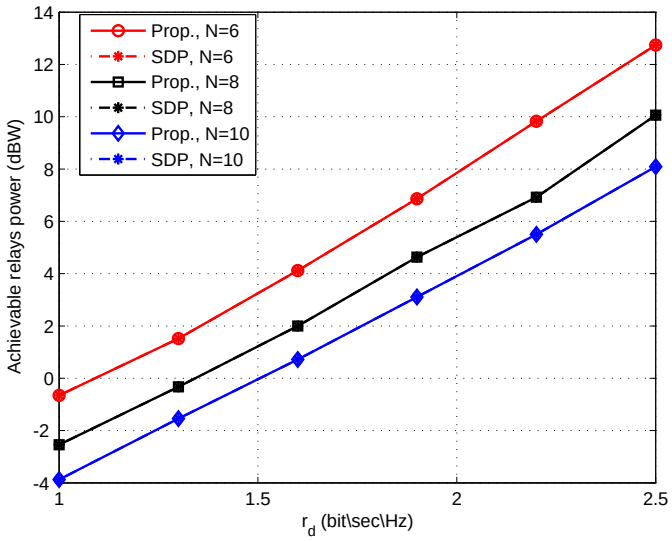

Figure 2.3: comparision of our Algorithm 2.3 that uses our proposed solution to find w and Algorithm 2.3 that uses SDP when both constraints are assumed to hold with equality with different number of relays, $\delta = 0.1$, and $P_1 = 15dBW$.

solution which means that our novel approach provides the optimal solution ($\mathbf{w}^*$) exactly as SDP. Also, it can be seen that the power of relays increases with the minimum destination information rate requirement. This is because increasing the required r_d needs to increase the power of relays to fulfill the requirements. It is also shown that increasing the number of relays improves the performance of the physical layer security system because of the array gain.

In Fig. 2.3, we implement a special case of our optimization problem where it is assumed that the information rates in both the destination and the eavesdropper must satisfy with equality; i.e., the exact r_d and r_e, where $\delta = 0.1$, and $P_1 = 15\ dBW$. In other words, we compare the SDP (2.17) with the proposed Algorithm 2.1. Similar to Fig. 2.2, the results in Fig. 2.3 show that for different number of relays and different minimum required information rate at destination, both

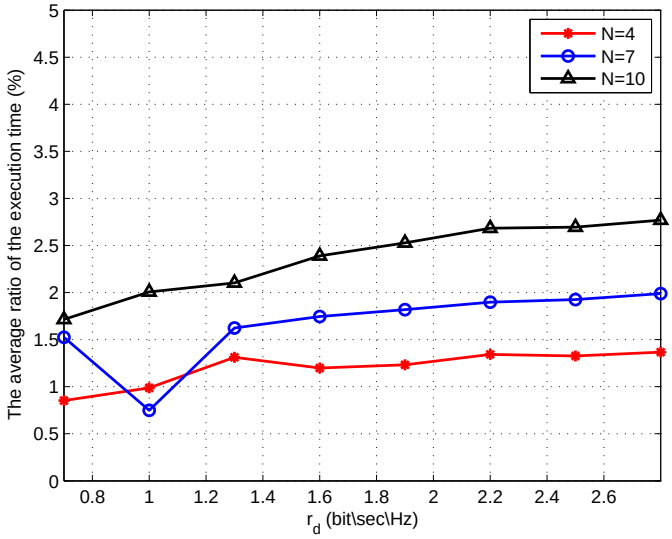

Figure 2.4: The average ratio of execution time spent by implementing our approach with relative SDP approach against the minimum required information rate at destination , N=4, N=7, N=10, $\delta = 0.1$ and $P_1 = 15dBW$

the SDP approach and our proposed algorithm provide the same optimal solution vector and the same relays transmit power.

In Fig. 2.4 we compare the computational complexity of SDP approach and our approach (Algorithm 2.2) in terms of the execution time. We plot the average percentage ratio of the execution time consumed by the proposed solution with respect to the SDP approach. It is shown that our algorithm provides substantially less computational complexity than the SDP approach where on average, it consumes only 1.7% of the time consumed by SDP which confirms what stated before that the complexity of implementing SDP is $O((M+N)^7)$, which is much more complex than implementing the eigenvalue problem that has $O(N^3)$ computational complexity.

Similarly, in Fig. 2.5, when both constraints are assumed to hold with equality,

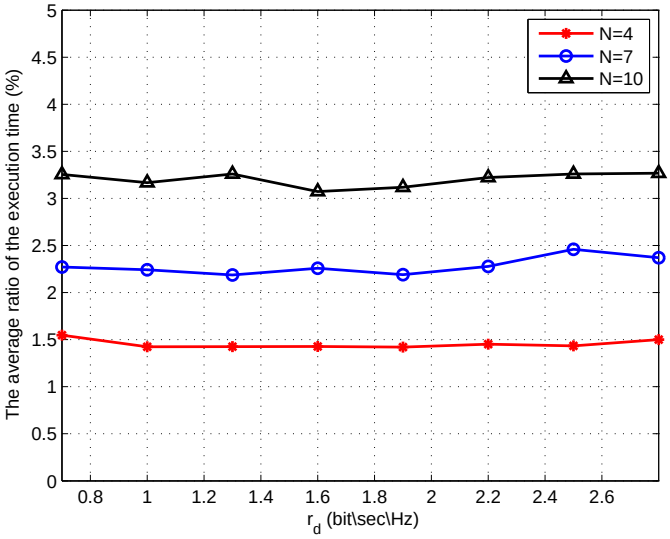

Figure 2.5: The average ratio of execution time spent by implementing our approach with relative SDP approach when both constraints hold with equality against the required minimum information rate at destination, N=4, N=7, N=10, $\delta = 0.1$ and $P_1 = 15\ dBW$.

we compare the computational complexity of the SDP approach and Algorithm 2.1 in terms of the execution time. We plot the average ratio of execution time consumed by the proposed solution with respect to the SDP approach. Although our Algorithm 2.1 proposes a series of eigenvalues problem to provide the optimal beamforming vector, it is shown that Algorithm 2.1 provides substantially less computational complexity than the SDP approach where, on average, consumes about 1.45%, 2.3%, and 3.2% of the time consumed by SDP in case of 4, 7, and 10 relays, respectively.

In Fig. 2.6, we show the relation of the achievable power of relays and the minimum destination information rate for a different values of the source power. As demonstrated before increasing the maximum available source power helps in decreasing the minimum required power of relays to satisfy the given rates. To

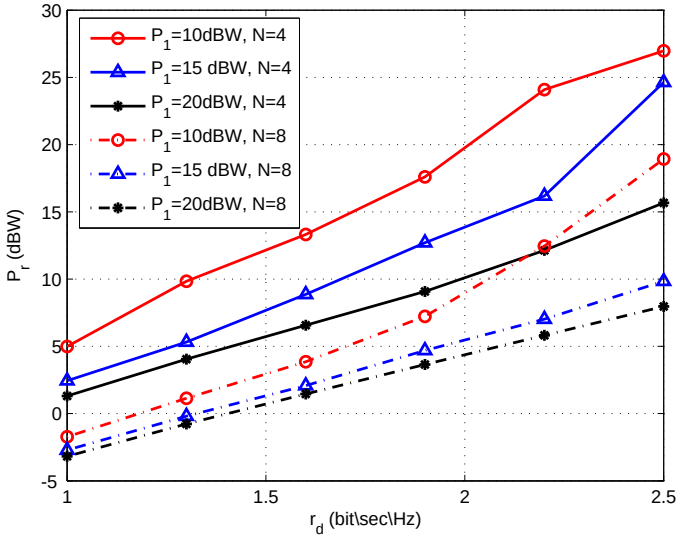

Figure 2.6: the relation of the achievable power of relays and the minimum destination information rate with a different values of of the source power.

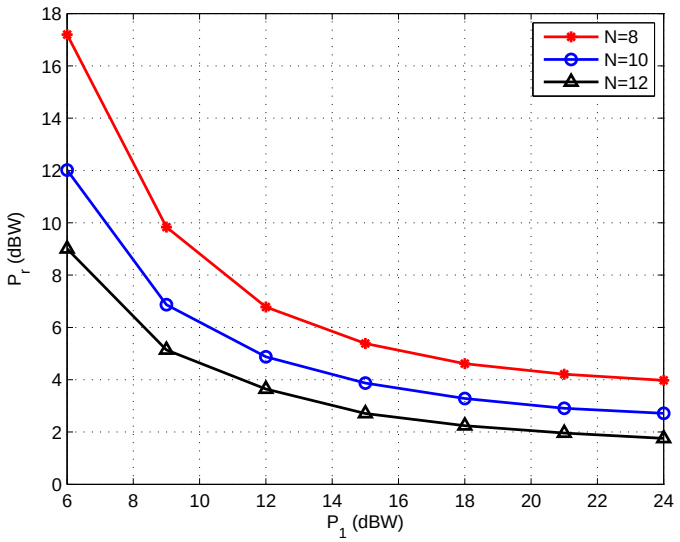

Figure 2.7: the power of relays against the total available power at source with various number of relays node.

show the relation between P_1 and the minimum required power of relays more clearly, we illustrate in Fig. 2.7 the power of relays versus the maximum available power at source with different number of relays node. We can see that the amount of enhancing the power of relays goes down as the power source increase. This is

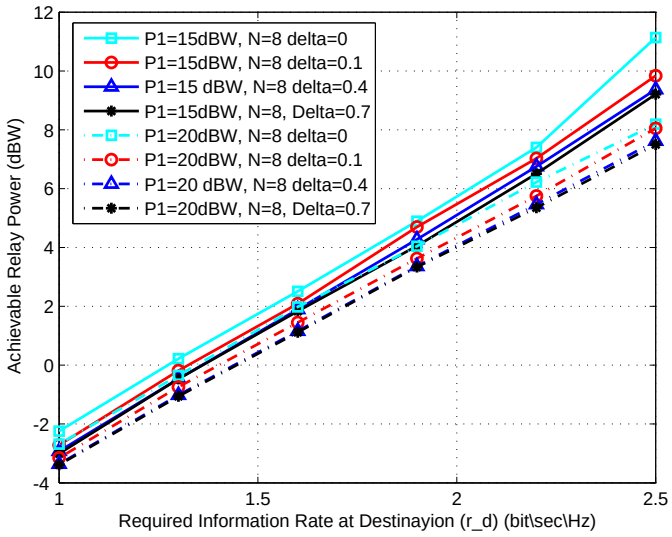

Figure 2.8: The achievable power of relays against the minimum requirement of the destination information rate with different values of δ

because as shown in the objective function of Problem (2.9) as the source power increases the rate of decreasing of the relaying power will decrease.

In Fig. 2.8, the achievable power of relays is plotted against the minimum requirement of the destination information rate with different values of δ (i.e., different values of r_e corresponds to r_d). It is shown that as δ increases, the achievable power of relays goes up. This is due to the reason that increasing r_e is freeing the objective function of Problem (2.9) to a certain degree. In other words, weakening the secrecy constraints helps in decreasing the required power of relays.

2.5 Conclusion

In this chapter, the physical layer security in a OWRS with several relays in the existence of an eavesdropper was investigated. The problem is formulated as minimizing the relaying power under information rate constraints. Then, the joint optimal solution source power and beamforming vector were obtained. A novel approach was proposed to solve the QCQP that also can be solved using SDP approach. The proposed algorithm provided the same optimal solution that can be achieved using SDP with dramatically reduced computational complexity. Furthermore, it was shown that increasing the maximum available source power helps in decreasing the minimum required relaying total power to satisfy the given rates.

CHAPTER 3

IMPROVING THE PHYSICAL LAYER SECURITY IN OWRS

3.1 Introduction

In this chapter, we improve the secure communications in OWRS by secrecy rate maximization when the total power has to be below a given value. We study the same system proposed in Chapter 1 with same specifications and constraints. Our goal in this chapter is to provide the optimal weight vector $\mathbf{w}$ that maximizes the secrecy rate. It is shown in the literature review that the secrecy rate maximization has been handled extensively, whereas the optimal beamforming vector has not provided yet. Therefore, we intend to find the optimal weight vector and compare it with the suboptimal solutions provided in the previous work. Firstly, we formulate the optimization problem with showing that it is non-convex. Then, we convert the problem from $N-$dimensional search to one-dimensional search

with a series of SDP problems. After that, we provide an efficient algorithm that guarantees the optimal solution with less complexity.

3.2 Problem Formulation

In this section, we formulate the optimization problem which provides the optimal weight vector to maximize the secrecy rate while keeping the total power under a predefined value. The optimization problem can be expressed as follows:

$$\max_{\mathbf{w}} \quad R_s \tag{3.1a}$$

$$s.t \quad \mathbf{w}^H \mathbf{T} \mathbf{w} + P_s \leq P_T, \tag{3.1b}$$

where R_s is given in (2.6), $\mathbf{T} = P_s R_{ff} + \sigma^2 \mathbf{I}_N$, where $R_{ff} = diag(\mathbf{f}_r^H) diag(\mathbf{f}_r)$, and P_T is total power available in the source and relays. Problem (3.1) is not convex optimization problem and it is hard to tackle. In the following we reformulate the problem as a convex with one dimensional search. It has been proved in [11] that the constraint (3.1b) holds with equality at optimality. Thus, the optimization problem to find the optimal weight vector for maximizing the secrecy rate can be written as:

$$\max_{\mathbf{w}} \quad \frac{1}{2} \log(1 + \frac{P_s \mathbf{w}^H \mathbf{R}_{fd} \mathbf{w}}{\sigma_D^2 + \sigma_R^2 \mathbf{w}^H \mathbf{R}_{gg} \mathbf{w}}) \tag{3.2a}$$

$$-\frac{1}{2} \log(1 + \frac{P_s \mathbf{w}^H \mathbf{R}_{fe} \mathbf{w}}{\sigma_E^2 + \sigma_R^2 \mathbf{w}^H \mathbf{R}_{ee} \mathbf{w}}) \tag{3.2b}$$

$$s.t \quad \mathbf{w}^H \mathbf{T} \mathbf{w} = P_r, \tag{3.2c}$$

where P_r is the total available power at relays; $Pr = P_T - P_s$. We can rewrite Problem (3.2) equivalently as follows:

$$\max_{\mathbf{w}} \quad \Big(\frac{\sigma_D^2+\sigma_R^2\mathbf{w}^H\mathbf{R}_{gg}\mathbf{w}+P_s\mathbf{w}^H\mathbf{R}_{fd}\mathbf{w}}{\sigma_D^2+\sigma_R^2\mathbf{w}^H\mathbf{R}_{gg}\mathbf{w}}\Big)\Big(\frac{\sigma_E^2+\sigma_R^2\mathbf{w}^H\mathbf{R}_{ee}\mathbf{w}}{\sigma_E^2+\sigma_R^2\mathbf{w}^H\mathbf{R}_{ee}\mathbf{w}+P_s\mathbf{w}^H\mathbf{R}_{fe}\mathbf{w}}\Big), \tag{3.3a}$$

$$s.t \qquad \mathbf{w}^H\mathbf{T}\mathbf{w} = P_r. \tag{3.3b}$$

Let's assume the unit norm complex vector $\bar{\mathbf{w}}$ such that $\mathbf{T}^{0.5}\mathbf{w} = \sqrt{P_r}\bar{\mathbf{w}}$. Hence $\bar{\mathbf{w}}^H\bar{\mathbf{w}} = \frac{\mathbf{w}^H\mathbf{T}\mathbf{w}}{P_r} = 1$, and $\mathbf{w} = \sqrt{P_r}\mathbf{T}^{-0.5}\bar{\mathbf{w}}$. Therefore, Problem (3.3) is equivalent to

$$\max_{\bar{\mathbf{w}}} \quad \frac{\bar{\mathbf{w}}^H(\sigma_D^2 + P_r\sigma_R^2\mathbf{T}^{-0.5}\mathbf{R}_{gg}\mathbf{T}^{-0.5} + P_sP_r\mathbf{T}^{-0.5}\mathbf{R}_{fd}\mathbf{T}^{-0.5})\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H(\sigma_1^2 + P_r\sigma^2\mathbf{T}^{-0.5}\mathbf{R}_{gg}\mathbf{T}^{-0.5})\bar{\mathbf{w}}}.$$
$$\frac{\bar{\mathbf{w}}^H(\sigma_E^2 + P_r\sigma_R^2\mathbf{T}^{-0.5}\mathbf{R}_{ee}\mathbf{T}^{-0.5})\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H(\sigma_E^2 + P_r\sigma_R^2\mathbf{T}^{-0.5}\mathbf{R}_{ee}\mathbf{T}^{-0.5} + P_sP_r\mathbf{T}^{-0.5}\mathbf{R}_{fe}\mathbf{T}^{-0.5})\bar{\mathbf{w}}} \tag{3.4a}$$

$$s.t \qquad \|\bar{\mathbf{w}}\|^2 = 1.$$

Let

$$\bar{\mathbf{A}}_1 = \sigma_D^2 + P_r\sigma_R^2\mathbf{T}^{-0.5}\mathbf{R}_{gg}\mathbf{T}^{-0.5} + P_sP_r\mathbf{T}^{-0.5}\mathbf{R}_{fd}\mathbf{T}^{-0.5},$$

$$\bar{\mathbf{A}}_2 = \sigma_D^2 + P_r\sigma^2\mathbf{T}^{-0.5}\mathbf{R}_{gg}\mathbf{T}^{-0.5},$$

$$\bar{\mathbf{A}}_3 = \sigma_E^2 + P_r\sigma_R^2\mathbf{T}^{-0.5}\mathbf{R}_{ee}\mathbf{T}^{-0.5},$$

$$\bar{\mathbf{A}}_4 = \sigma_E^2 + P_r\sigma_R^2\mathbf{T}^{-0.5}\mathbf{R}_{ee}\mathbf{T}^{-0.5} + P_sP_r\mathbf{T}^{-0.5}\mathbf{R}_{fe}\mathbf{T}^{-0.5}.$$

Therefore, we can rewrite Problem (3.4) as follows:

$$\max_{\bar{\mathbf{w}}} \quad \frac{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_1 \bar{\mathbf{w}}}{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_2 \bar{\mathbf{w}}} . \frac{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_3 \bar{\mathbf{w}}}{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_4 \bar{\mathbf{w}}} \tag{3.5a}$$

$$s.t \quad \|\bar{\mathbf{w}}\|^2 = 1. \tag{3.5b}$$

The constraint (3.5b) does not have an effect on the objective function value because the maximum value of the objective function will be the same whatever the norm of the vector is. Therefore, we can remove (3.5b) without affecting the solution of Problem (3.5). After we get the optimal $\bar{\mathbf{w}}$, we normalize it. Although it is hard to find the optimal solution of the product of two Rayleigh quotients (RQ), in the following we obtain the optimal solution for Problem (3.5) by reformulating the problem into SDP with one dimensional search. We have that $\lambda_{min}(\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3) \leq \frac{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_3 \bar{\mathbf{w}}}{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_4 \bar{\mathbf{w}}} \leq \lambda_{max}(\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3)$, where $\lambda_{min}(\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3)$ is the minimum eigenvalue of the matrix $\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3$, and $\lambda_{max}(\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3)$ is the largest eigenvalue of the matrix $\lambda_{max}(\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3)$. Let's denote the product of two RQs function by $R_q(\bar{\mathbf{w}}) = \frac{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_1 \bar{\mathbf{w}}}{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_2 \bar{\mathbf{w}}} . \frac{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_3 \bar{\mathbf{w}}}{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_4 \bar{\mathbf{w}}}$, or $R_q(\bar{\mathbf{w}}) = u_1 u_2$, where $u_1 = \frac{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_1 \bar{\mathbf{w}}}{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_2 \bar{\mathbf{w}}}$, and $u_2 = \frac{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_3 \bar{\mathbf{w}}}{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_4 \bar{\mathbf{w}}}$. To obtain the optimal values u_1 and u_2, we start by maximizing one of them while fixing the other. Let's rewrite the optimization problem (3.5) as follows:

$$\max_{\bar{\mathbf{w}}} \quad \frac{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_1 \bar{\mathbf{w}}}{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_2 \bar{\mathbf{w}}} \tag{3.6a}$$

$$s.t \quad \frac{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_3 \bar{\mathbf{w}}}{\bar{\mathbf{w}}^H \bar{\mathbf{A}}_4 \bar{\mathbf{w}}} = u_2. \tag{3.6b}$$

The expression $\bar{\mathbf{w}}^H \bar{\mathbf{A}}_2 \bar{\mathbf{w}}$ is considered as a normalizing vector that can be converted to a constraint $\bar{\mathbf{w}}^H \bar{\mathbf{A}}_2 \bar{\mathbf{w}} = 1$. Therefore, Problem (3.6) can be written as follows:

$$\max_{\bar{\mathbf{w}}} \quad \bar{\mathbf{w}}^H \bar{\mathbf{A}}_1 \bar{\mathbf{w}} \tag{3.7a}$$

$$s.t. \quad \bar{\mathbf{w}}^H \bar{\mathbf{A}}_3 \bar{\mathbf{w}} - u_2 \bar{\mathbf{w}}^H \bar{\mathbf{A}}_4 \bar{\mathbf{w}} \geq 0 \tag{3.7b}$$

$$\bar{\mathbf{w}}^H \bar{\mathbf{A}}_2 \bar{\mathbf{w}} = 1. \tag{3.7c}$$

Problem (3.7) is a non-convex QCQP which is not easy to tackle. To solve problem (3.7) we have to transform it into SDP with rank one constraint by introducing the new variable $\bar{\mathbf{Q}} = \bar{\mathbf{w}}\bar{\mathbf{w}}^H$. Now, Problem (3.7) can be written as:

$$\max_{\bar{\mathbf{Q}}} \quad tr(\bar{\mathbf{A}}_1 \bar{\mathbf{Q}}) \tag{3.8a}$$

$$s.t \quad tr(\bar{\mathbf{A}}_3 \bar{\mathbf{Q}}) - u_2 tr(\bar{\mathbf{A}}_4 \bar{\mathbf{Q}}) = 0 \tag{3.8b}$$

$$tr(\bar{\mathbf{A}}_2 \bar{\mathbf{Q}}) = 1 \tag{3.8c}$$

$$\bar{\mathbf{Q}} \succeq 0, \qquad Rank(\bar{\mathbf{Q}}) = 1 \tag{3.8d}$$

The constraint in (3.8d) guarantees that the matrix $\bar{\mathbf{Q}}$ can be written as $\bar{\mathbf{Q}} = \bar{\mathbf{w}}\bar{\mathbf{w}}^H$. Problem (3.8) is also not convex because the rank constraint of $\bar{\mathbf{Q}}$. In [41], it is shown that if the number of the trace constraints is n, we can obtain a global optimal solution with rank $r \leq \sqrt{n}$. Here in Problem (3.8), number of trace constraints is two traces which means that the solution matrix is rank one.

Therefore, Problem (3.8) is equivalent to the following convex problem:

$$\max_{\bar{\mathbf{Q}}} \quad tr(\bar{\mathbf{A}}_1\bar{\mathbf{Q}}) \tag{3.9a}$$

$$s.t \quad tr(\bar{\mathbf{A}}_3\bar{\mathbf{Q}}) - u_2 tr(\bar{\mathbf{A}}_4\bar{\mathbf{Q}}) = 0 \tag{3.9b}$$

$$tr(\bar{\mathbf{A}}_2\bar{\mathbf{Q}}) = 1 \tag{3.9c}$$

$$\bar{\mathbf{Q}} \succeq 0. \tag{3.9d}$$

Problem (3.9) indicates that if we have the optimal value of u_2 that maximize $R_q(\bar{\mathbf{w}})$, we can find the optimal value of u_1. Let's denote the optimal value of u_2 and u_1 that maximize the function $R_q(\bar{\mathbf{w}})$ by u_2^* and u_1^*, respectively. Therefore, our problem now is to search for the optimal value u_2^* that maximizes $R_q(\bar{\mathbf{w}})$. As stated earlier: $\lambda_{min}(\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3) \leq u_2^* \leq \lambda_{max}(\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3)$. If we choose $\bar{\mathbf{w}}$ to be the eigenvector related to the largest eigenvalue of the principle matrix $(\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3)$; i.e., $\bar{\mathbf{w}} = \mathbf{v}_{max}(\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3)$, the objective function $R_q(\bar{\mathbf{w}})$ will be $R_q(\bar{\mathbf{w}}) = \frac{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_2\bar{\mathbf{w}}}\lambda_{max}(\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3)$. Define $\lambda_{34} = \lambda_{max}(\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3)$, $\lambda_{12} = \lambda_{max}(\bar{\mathbf{A}}_2^{-1}\bar{\mathbf{A}}_1)$, σ_{34} is the maximum value of $\frac{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_3\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_4\bar{\mathbf{w}}}$ when $\frac{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_2\bar{\mathbf{w}}} = \lambda_{12}$, and σ_{12} is the maximum value of $\frac{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_2\bar{\mathbf{w}}}$ when $\frac{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_3\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_4\bar{\mathbf{w}}} = \lambda_{34}$. To obtain the value of σ_{12} we have two cases: the first case if the $\lambda_{max}(\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3)$ is unique (i.e., $\lambda_{max}(\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3)$ is distinct), we will choose $\bar{\mathbf{w}}$ to be the eigenvector associated $\lambda_{max}(\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3)$ and $\sigma_{12} = \frac{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_2\bar{\mathbf{w}}}$. The second case if the matrix $\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3$ has another eigenvalue equals to $\lambda_{max}(\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3)$ (i.e., the maximum eigenvalue of matrix $\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3$ is not unique), we have to obtain the maximum value of σ_{12} by solving the SDP (3.9) when $u_2 = \lambda_{max}(\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3)$. Similarly, we can obtain σ_{34}. Consequently, u_1 cannot reach its maximum value

if $u_2 > \sigma_{34}$. In problem (3.9), if we put $u_2 = \lambda_{34}$, the function $R_q(\bar{\mathbf{w}})$ will be equal to $\sigma_{12}\lambda_{34}$. On the other hand, if we put $u_2 = \sigma_{34}$, u_1 will reach its maximum value λ_{12} then $R_q(\bar{\mathbf{w}}) = \sigma_{34}\lambda_{12}$. While the maximum value of the function is $R_q(\bar{\mathbf{w}}) \geq \max(\sigma_{12}\lambda_{34}, \sigma_{34}\lambda_{12})$. It can be shown that the optimal value of u_2^* cannot be less than σ_{34}. This is because as we decrease u_2 below σ_{34}, u_1 will be less than or equal to its maximum value, while u_2 will keep decreasing which means that the product of them will be definitely less than $\sigma_{34}\lambda_{12}$. Consequently, u_2^* is bounded by $\sigma_{34} \leq u_2^* \leq \lambda_{34}$. Similarly $\sigma_{12} \leq u_1^* \leq \lambda_{12}$.

Lemma 3.1 *Problem (3.9) is equivalent to the following problem:*

$$\max_{\bar{\mathbf{Q}}} \quad tr(\bar{\mathbf{A}}_1\bar{\mathbf{Q}}) \tag{3.10a}$$

$$s.t \quad tr(\bar{\mathbf{A}}_3\bar{\mathbf{Q}}) - u_2 tr(\bar{\mathbf{A}}_4\bar{\mathbf{Q}}) = 0 \tag{3.10b}$$

$$tr(\bar{\mathbf{A}}_2\bar{\mathbf{Q}}) \leq 1 \tag{3.10c}$$

$$\bar{\mathbf{Q}} \succeq 0, \tag{3.10d}$$

Proof. It can be shown that the optimal solution of (3.10) must satisfy the constraint (3.10c) with equality and hence it will be the same optimal solution of (3.9). This is because if the solution of (3.10) satisfies (3.10c) with strict inequality, we can always multiply $\bar{\mathbf{Q}}$ by a constant $\beta > 1$ to satisfy (3.10c) with equality while increasing the objective function; since $tr(\bar{\mathbf{A}}_1\bar{\mathbf{Q}}) < tr(\beta\bar{\mathbf{A}}_1\bar{\mathbf{Q}})$. Also, the constraints (3.10b) and (3.10d) will remain satisfied; since $tr(\bar{\mathbf{A}}_3\bar{\mathbf{Q}}) - u_2 tr(\bar{\mathbf{A}}_4\bar{\mathbf{Q}})) = \beta tr(\bar{\mathbf{A}}_3\bar{\mathbf{Q}}) - u_2 tr(\bar{\mathbf{A}}_4\bar{\mathbf{Q}}) = 0$. ∎

Lemma 3.2 *If* $(u_2 > \sigma_{34})$*, problem (3.10) is equivalent to the following problem:*

$$\max_{\bar{\mathbf{Q}}} \quad tr(\bar{\mathbf{A}}_1\bar{\mathbf{Q}}) \tag{3.11a}$$

$$s.t \quad tr(\bar{\mathbf{A}}_3\bar{\mathbf{Q}}) - u_2 tr(\bar{\mathbf{A}}_4\bar{\mathbf{Q}}) \geq 0 \tag{3.11b}$$

$$tr(\bar{\mathbf{A}}_2\bar{\mathbf{Q}}) \leq 1 \tag{3.11c}$$

$$\bar{\mathbf{Q}} \succeq 0, \tag{3.11d}$$

Proof. Problem (3.11) is convex considering that the objective and the constraint functions are convex. It can also be shown that the problem in (3.11) satisfies Slater's condition which states that the strong duality holds if there exists a feasible point at which the inequality constraints hold with strict inequalities and the primal optimization problem is also convex (details in [42]). Thus, the KKT conditions are sufficient and necessary for a primal-dual point to be optimal. The Lagrangian function of problem (3.11) is

$$\begin{aligned}\Gamma = &- tr(\bar{\mathbf{A}}_1\bar{\mathbf{Q}})) - tr(\bar{\mathbf{Q}}\mathbf{Q}) + \beta_0 tr(\bar{\mathbf{A}}_2\bar{\mathbf{Q}})) - \beta_1 tr(\bar{\mathbf{A}}_3\bar{\mathbf{Q}}) \\ &+ \beta_1 u_2 tr(\bar{\mathbf{A}}_4\bar{\mathbf{Q}}) - \beta_0,\end{aligned} \tag{3.12}$$

where $\beta_0 \geq 0, \beta_1 \geq 0$ and $\mathbf{Q} \succeq 0$ are the Lagrangian dual variables. Define $\bar{\mathbf{w}}^o$, β_0^o and β_1^o are the optimal primal and dual solutions when u_2 is given, while $\bar{\mathbf{w}}^*$, β_0^* and β_1^* are the primal and dual optimal solutions when u_2 is the optimal value that maximize the $R_q(\bar{\mathbf{w}})$ function; i.e., $u_2 = u_2^*$.

Hence, the KKT conditions for a given u_2 are:

$$\frac{d\Gamma}{d\bar{\mathbf{Q}}} = \bar{\mathbf{A}}_1 - \mathbf{Q}^o + \beta_0^o \bar{\mathbf{A}}_2 + \beta_1^o(u_2\bar{\mathbf{A}}_4 - \bar{\mathbf{A}}_3) = 0 \tag{3.13a}$$

$$tr(\bar{\mathbf{Q}}^o\bar{\mathbf{A}}_2) - 1 \geq 0 \tag{3.13b}$$

$$tr(\bar{\mathbf{Q}}^o(\bar{\mathbf{A}}_3 - u_2\bar{\mathbf{A}}_4)) \geq 0 \tag{3.13c}$$

$$tr(\bar{\mathbf{Q}}^o\mathbf{Q}^{\mathbf{o}}) = 0 \tag{3.13d}$$

$$\beta_0^o tr(\bar{\mathbf{Q}}^o\bar{\mathbf{A}}_2) - \beta_0^o = 0 \tag{3.13e}$$

$$\beta_1^o tr(\bar{\mathbf{Q}}^o(\bar{\mathbf{A}}_3 - u_2\bar{\mathbf{A}}_4)) - \beta_1^o = 0 \tag{3.13f}$$

$$\bar{\mathbf{Q}}^{\mathbf{o}} \succeq 0, \quad \mathbf{Q}^o \succeq 0 \quad \beta_0^o \geq 0 \quad \beta_1^o \geq 0. \tag{3.13g}$$

From (3.13a), the dual optimization problem can be written as follows:

$$\min_{\beta_0,\beta_1} \quad \beta_0 \tag{3.14a}$$

$$s.t. \quad -\bar{\mathbf{A}}_1 + \beta_0\bar{\mathbf{A}}_2 + \beta_1(u_2\bar{\mathbf{A}}_4 - \bar{\mathbf{A}}_3) \succcurlyeq 0, \tag{3.14b}$$

$$\beta_0 \geq 0, \beta_1 \geq 0. \tag{3.14c}$$

Since strong duality holds,

$$\beta_0^o = tr(\bar{\mathbf{A}}_1\bar{\mathbf{Q}}^o) = u_1 = \frac{tr(\bar{\mathbf{A}}_1\bar{\mathbf{Q}}^o)}{tr(\bar{\mathbf{A}}_2\bar{\mathbf{Q}}^o)} \leq \lambda_{12}. \tag{3.15}$$

From the constraint (3.14b), If we set $\beta_1 = 0$, β_0 will be equal to $\lambda_{max}(\bar{\mathbf{A}}_2^{-1}\bar{\mathbf{A}}_1) = \lambda_{12}$ which is its maximum value, which means that $u_2 = \sigma_{34}$. Therefore, if $u_2 > \sigma_{34}$ then β_1^* cannot be zero. Therefore, from the constraint (3.14c), we have $\beta_1^o > 0$.

From the KKT condition (3.13f), if $\beta_1^o > 0$, then $tr(\bar{\mathbf{A}}_3\bar{\mathbf{Q}}^o) - u_2 tr(\bar{\mathbf{A}}_4\bar{\mathbf{Q}}^o) = 0$, which means that the constraint (3.11b) holds with equality. As a result, problem (3.11) and (3.10) are equivalent. ∎

In case $u_2 = \sigma_{34}$, β_0^o will reach its maximum value and $u_1 = \lambda_{12}$. In the following, we propose an algorithm that guarantees the global optimal solution of the $R_q(\bar{\mathbf{w}})$.

Algorithm 3.1 Finding the optimal null space beamforming vector $\bar{\mathbf{q}}$ by series of SDPs

---

set $u_2 = u_2^{(0)} : \Delta u_2 : u_2^{(m)}$, and implement the SDP (3.11) with each value of u_2 to achieve the maximum value of $R_q(\bar{\mathbf{w}})$, where $u_2^{(0)} = \sigma_{34}$, and $u_2^{(m)} = \lambda_{34}$, and Δu_2 is the step size.

This algorithm is highly complex since we need to implement $\lfloor \frac{\lambda_{34}-\sigma_{34}}{\Delta u_2} \rfloor$ SDP's and we should have the value of Δu_2 very small to obtain accurate optimal solution. We can adopt it as a benchmark to test if we achieve the optimal value or not. Usually, interior point method is used to solve the SDP problems. Implementing only one SDP is not considerd highly complex despite it needs $O((M+N)^7)$ in the computational complexity, where M is the number of the traces constraint and N is the dimension of the column or the row in $\bar{\mathbf{A}}_1$ (number of relays). From problem (3.14), we can rewrite the constraint (3.14b) as

$$\beta_0\bar{\mathbf{A}}_2 \succcurlyeq \bar{\mathbf{A}}_1 + \beta_1\bar{\mathbf{A}}_3 - \beta_1 u_2\bar{\mathbf{A}}_4.$$

Because $\bar{\mathbf{A}}_2$ is a positive definite matrix, then

$$\beta_0\mathbf{I} \succcurlyeq \bar{\mathbf{A}}_2^{-1}(\bar{\mathbf{A}}_1 + \beta_1\bar{\mathbf{A}}_3 - \beta_1 u_2\bar{\mathbf{A}}_4). \tag{3.16}$$

From (3.16) and the optimization problem (3.14), we can express β_0 as

$$\beta_0^o = \min_{\beta_1} \lambda_{max}(\bar{\mathbf{A}}_2^{-1}(\bar{\mathbf{A}}_1 + \beta_1\bar{\mathbf{A}}_3 - \beta_1 u_2\bar{\mathbf{A}}_4)) \tag{3.17}$$

Let $\mathbf{y} = \mathbf{v}_{max}(\bar{\mathbf{A}}_2^{-1}(\bar{\mathbf{A}}_1 + \beta_1^o\bar{\mathbf{A}}_3 - \beta_1^o u_2\bar{\mathbf{A}}_4))$ which means that

$$\begin{aligned}\beta_0^o &= \mathbf{y}^H(\bar{\mathbf{A}}_2^{-1}(\bar{\mathbf{A}}_1 + \beta_1^o\bar{\mathbf{A}}_3 - \beta_1^o u_2\bar{\mathbf{A}}_4))\mathbf{y} \\ &= \frac{\mathbf{y}^H\bar{\mathbf{A}}_1\mathbf{y}}{\mathbf{y}^H\bar{\mathbf{A}}_2\mathbf{y}} + \beta_1^o\frac{\mathbf{y}^H\bar{\mathbf{A}}_3\mathbf{y}}{\mathbf{y}^H\bar{\mathbf{A}}_2\mathbf{y}} - \beta_1^o u_2\frac{\mathbf{y}^H\bar{\mathbf{A}}_4\mathbf{y}}{\mathbf{y}^H\bar{\mathbf{A}}_2\mathbf{y}}.\end{aligned} \tag{3.18}$$

From the condition (3.13f) and Lemma 3.2, at the optimality of problem (3.14), β_1^o must be selected to satisfy that $\bar{\mathbf{w}}^{oH}\bar{\mathbf{A}}_3\bar{\mathbf{w}}^o - u_2\bar{\mathbf{w}}^{oH}\bar{\mathbf{A}}_4\bar{\mathbf{w}}^o = 0$. Therefore, from (3.15), we can rewrite β_0^o as

$$\beta_0^o = \frac{\bar{\mathbf{w}}^{oH}\bar{\mathbf{A}}_1\bar{\mathbf{w}}^o}{\bar{\mathbf{w}}^{oH}\bar{\mathbf{A}}_2\bar{\mathbf{w}}^o} + \underbrace{\beta_1^o\frac{\bar{\mathbf{w}}^{oH}\bar{\mathbf{A}}_3\bar{\mathbf{w}}^o - u_2\bar{\mathbf{w}}^{oH}\bar{\mathbf{A}}_4\bar{\mathbf{w}}^o}{\bar{\mathbf{w}}^{oH}\bar{\mathbf{A}}_2\bar{\mathbf{w}}^o}}_{=0} \tag{3.19}$$

From (3.18) and (3.19), we can show that the optimal solution vector of Problem (3.9) is

$$\bar{\mathbf{w}}^o = \mathbf{y} = \mathbf{v}_{max}(\bar{\mathbf{A}}_2^{-1}(\bar{\mathbf{A}}_1 + \beta_1^o\bar{\mathbf{A}}_3 - \beta_1^o u_2\bar{\mathbf{A}}_4)). \tag{3.20}$$

For a given u_2, Problem (3.17) is a convex problem (details in [42]). Hence, we use the bisection algorithm to obtain the optimal $\bar{\mathbf{w}}^o$ where β_1^o is selected to satisfy that $\bar{\mathbf{w}}^{oH}\bar{\mathbf{A}}_3\bar{\mathbf{w}}^o = u_2\bar{\mathbf{w}}^{oH}\bar{\mathbf{A}}_4\bar{\mathbf{w}}^o$ (aiming to satisfy the condition (3.13f)) with a given u_2.

β_{1min} and β_{1max} should be determined to achieve that

Algorithm 3.2 Obtain $\bar{\mathbf{w}}^o$ with a given u_2

1. Determine the maximum and minimum value of β_1; i.e., define β_{1min} and β_{1max} (finding β_{1max} and β_{1min} is explained after).
2. Let $\beta = (\beta_{1min} + \beta_{1max})/2$, then find $\bar{\mathbf{w}} = \mathbf{v}_{max}(\bar{\mathbf{A}}_2^{-1}(\bar{\mathbf{A}}_1 + \beta\bar{\mathbf{A}}_3 - \beta u_2\bar{\mathbf{A}}_4))$.
3. If $\bar{\mathbf{w}}^H\bar{\mathbf{A}}_3\bar{\mathbf{w}} < u_2\bar{\mathbf{w}}^H\bar{\mathbf{A}}_4\bar{\mathbf{w}}$, $\beta_{1max} = \beta$, else if $\bar{\mathbf{w}}^H\bar{\mathbf{A}}_3\bar{\mathbf{w}} > u_2\bar{\mathbf{w}}^H\bar{\mathbf{A}}_4\bar{\mathbf{w}}$, $\beta_{1min} = \beta$.
4. If $|\bar{\mathbf{w}}^H\bar{\mathbf{A}}_3\bar{\mathbf{w}} - u_2\bar{\mathbf{w}}^H\bar{\mathbf{A}}_4\bar{\mathbf{w}}| \leq \varepsilon$, $\beta_1^o = (\beta_{1min} + \beta_{1max})/2$, otherwise go back to step 2.
5. Find $\bar{\mathbf{w}}^o = \mathbf{v}_{max}(\bar{\mathbf{A}}_2^{-1}(\bar{\mathbf{A}}_1 + \beta_1^o\bar{\mathbf{A}}_3 - \beta_1^o u_2\bar{\mathbf{A}}_4))$.

$\bar{\mathbf{w}}^H(\beta_{1min})\bar{\mathbf{A}}_3\bar{\mathbf{w}}(\beta_{1min}) < u_2\bar{\mathbf{w}}^H(\beta_{1min})\bar{\mathbf{A}}_4\bar{\mathbf{w}}(\beta_{1min})$ and $\bar{\mathbf{w}}^H(\beta_{1max})\bar{\mathbf{A}}_3\bar{\mathbf{w}}(\beta_{1max}) > u_2\bar{\mathbf{w}}^H(\beta_{1max})\bar{\mathbf{A}}_4\bar{\mathbf{w}}(\beta_{1max})$; i.e, there is a cross point between β_{1min} and β_{1max} which guarantees that $\bar{\mathbf{w}}^H\bar{\mathbf{A}}_3\bar{\mathbf{w}} = u_2\bar{\mathbf{w}}^H\bar{\mathbf{A}}_4\bar{\mathbf{w}}$.

Algorithm 3.2 is much simpler than implementing one SDP problem since the implementing of the eigenvalue problem needs only to $O(N^3)$ computational complexity. Therefor we can adopt Algorithm 3.2 instead of implementing SDP problems for all possible values of u_2. It guarantees the optimal solution, but we intend to simplify it more. In the following, we propose a novel efficient algorithm to provide the optimal $\bar{\mathbf{w}}^*$ that maximizes the objective function of Problem (3.5).

Since $\beta_0^o = u_1$, we can claim that expression (3.17) is an expressing u_1 in terms of u_2. Hence, we can rewrite the optimization problem (3.5) as follows:

$$\begin{aligned}\max_{u_2} \beta_0^o u_2 &= \max_{u_2} \min_{\beta_1} \lambda_{max}(\bar{\mathbf{A}}_2^{-1}(u_2\bar{\mathbf{A}}_1 + u_2\beta_1\bar{\mathbf{A}}_3 - \beta_1 u_2^2\bar{\mathbf{A}}_4) \\ &= \max_{u_2} \bar{\mathbf{w}}^{oH}(\bar{\mathbf{A}}_2^{-1}(u_2\bar{\mathbf{A}}_1 + u_2\beta_1^o\bar{\mathbf{A}}_3 - \beta_1^o u_2^2\bar{\mathbf{A}}_4)\bar{\mathbf{w}}^o\end{aligned} \tag{3.21}$$

Lemma 3.3 *At the optimality of Problem (3.5), we have* $\beta_1^* = \frac{\bar{\mathbf{w}}^{*H}\bar{\mathbf{A}}_1\bar{\mathbf{w}}^*}{u_2^*\bar{\mathbf{w}}^{*H}\bar{\mathbf{A}}_4\bar{\mathbf{w}}^*}$.

Proof. At the optimality, we have that

$$\beta_0^* u_2^* = \frac{\bar{\mathbf{w}}^{*H}\bar{\mathbf{A}}_1\bar{\mathbf{w}}^*}{\bar{\mathbf{w}}^{*H}\bar{\mathbf{A}}_2\bar{\mathbf{w}}^*}.\frac{\bar{\mathbf{w}}^{*H}\bar{\mathbf{A}}_3\bar{\mathbf{w}}^*}{\bar{\mathbf{w}}^{*H}\bar{\mathbf{A}}_4\bar{\mathbf{w}}^*}, \tag{3.22}$$

and from equation (3.21)

$$\begin{aligned}\beta_0^* u_2^* &= \bar{\mathbf{w}}^{*H}(\bar{\mathbf{A}}_2^{-1}(u_2^*\bar{\mathbf{A}}_1 + u_2^*\beta_1^*\bar{\mathbf{A}}_3 - \beta_1^* u_2^{*2}\bar{\mathbf{A}}_4)\bar{\mathbf{w}}^* \\ &= u_2^*\frac{\bar{\mathbf{w}}^{*H}\bar{\mathbf{A}}_1\bar{\mathbf{w}}^*}{\bar{\mathbf{w}}^{*H}\bar{\mathbf{A}}_2\bar{\mathbf{w}}^*} + u_2^*\beta_1^*\frac{\bar{\mathbf{w}}^{*H}\bar{\mathbf{A}}_3\bar{\mathbf{w}}^* - u_2^*\bar{\mathbf{w}}^{*H}\bar{\mathbf{A}}_4\bar{\mathbf{w}}^*}{\bar{\mathbf{w}}^{*H}\bar{\mathbf{A}}_2\bar{\mathbf{w}}^*}\end{aligned} \tag{3.23}$$

It is obvious that the left hand side of equation (3.23) is equal to the right hand side of that equation when $\beta_1^* = \frac{\bar{\mathbf{w}}^{*H}\bar{\mathbf{A}}_1\bar{\mathbf{w}}^*}{u_2^*\bar{\mathbf{w}}^{*H}\bar{\mathbf{A}}_4\bar{\mathbf{w}}^*} = \frac{\bar{\mathbf{w}}^{*H}\bar{\mathbf{A}}_1\bar{\mathbf{w}}^*}{\bar{\mathbf{w}}^{*H}\bar{\mathbf{A}}_3\bar{\mathbf{w}}^*}$. ∎

Consequently, we will exploit Lemma 3 to propose an efficient novel algorithm that guarantees the optimal $\bar{\mathbf{w}}^*$ with very less complexity.

From Lemma 3.3, we have $\lambda_{min}(\bar{\mathbf{A}}_3^{-1}\bar{\mathbf{A}}_1) \leq \beta_1^* \leq \lambda_{max}(\bar{\mathbf{A}}_3^{-1}\bar{\mathbf{A}}_1)$. We can reduce the search space of β_1^* similar as we did for u_2^*. From the fact that $\sigma_{34} \leq u_2^* \leq \lambda_{34}$, we have the maximum and minimum values of $\bar{\mathbf{w}}^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}$ are $\bar{\mathbf{w}}_1^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}_1$ and $\bar{\mathbf{w}}_2^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}_2$, respectively, where $\bar{\mathbf{w}}_1 = \mathbf{v}_{max}(\bar{\mathbf{A}}_2^{-1}\bar{\mathbf{A}}_1)$ and $\bar{\mathbf{w}}_2 = \mathbf{v}_{max}(\bar{\mathbf{A}}_4^{-1}\bar{\mathbf{A}}_3)$. Similarly, the maximum and minimum values of $\bar{\mathbf{w}}^H\bar{\mathbf{A}}_3\bar{\mathbf{w}}$ are $\bar{\mathbf{w}}_2^H\bar{\mathbf{A}}_3\bar{\mathbf{w}}_2$ and $\bar{\mathbf{w}}_1^H\bar{\mathbf{A}}_3\bar{\mathbf{w}}_1$, respectively. Consequently,

$$\min(\frac{\bar{\mathbf{w}}_1^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}_1}{\bar{\mathbf{w}}_1^H\bar{\mathbf{A}}_3\bar{\mathbf{w}}_1}, \frac{\bar{\mathbf{w}}_2^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}_2}{\bar{\mathbf{w}}_2^H\bar{\mathbf{A}}_3\bar{\mathbf{w}}_2}) \leq \beta_1^* \leq \max(\frac{\bar{\mathbf{w}}_1^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}_1}{\bar{\mathbf{w}}_1^H\bar{\mathbf{A}}_3\bar{\mathbf{w}}_1}, \frac{\bar{\mathbf{w}}_2^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}_2}{\bar{\mathbf{w}}_2^H\bar{\mathbf{A}}_3\bar{\mathbf{w}}_2}). \tag{3.24}$$

Let $\lambda_{13} = \max(\frac{\bar{\mathbf{w}}_1^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}_1}{\bar{\mathbf{w}}_1^H\bar{\mathbf{A}}_3\bar{\mathbf{w}}_1}, \frac{\bar{\mathbf{w}}_2^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}_2}{\bar{\mathbf{w}}_2^H\bar{\mathbf{A}}_3\bar{\mathbf{w}}_2})$, and $\sigma_{13} = \min(\frac{\bar{\mathbf{w}}_1^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}_1}{\bar{\mathbf{w}}_1^H\bar{\mathbf{A}}_3\bar{\mathbf{w}}_1}, \frac{\bar{\mathbf{w}}_2^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}_2}{\bar{\mathbf{w}}_2^H\bar{\mathbf{A}}_3\bar{\mathbf{w}}_2})$. Thus, the algorithm to obtain the null space beamforming vector is

Algorithm 3.3 Finding the optimal vector that maximize the product of two RQ.

1. Give β_1 any value between σ_{13} and λ_{13}.
2. Search for u_2 between σ_{34} and λ_{34} that maximize $\frac{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_2\bar{\mathbf{w}}}.\frac{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_3\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_4\bar{\mathbf{w}}}$, where $\bar{\mathbf{w}} = \mathbf{v}_{max}(\bar{\mathbf{A}}_2^{-1}(u_2\bar{\mathbf{A}}_1 + u_2\beta_1\bar{\mathbf{A}}_3 - \beta_1 u_2^2\bar{\mathbf{A}}_4)$. (the procedures to look for u_2 are summarized below).
3. Define a new value for $\beta_1 = \frac{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}}{u_2\bar{\mathbf{w}}^H\bar{\mathbf{A}}_4\bar{\mathbf{w}}}$
4. Back to step (2) until the value of u_2 cannot improve the $R_q(\bar{\mathbf{w}})$ anymore.

Algorithm 3.3 is based on enforcing the value of β_1 to rapidly approach its optimal value by implementing Step 3. To implement Step 2 of Algorithm 3.3, we cannot use the bisection algorithm or any algorithm that is usually used for the convex problems because of the non-convexity of the original problem. However, due to the simplicity of implementing the eigenvalue problem compared to SDP since its complexity is $O(N^3)$ which is much simpler than SDP approach, exhaustive search might be suitable to look for the optimal u_2 or we can adopt the simple traditional random search algorithm [43] to look for u_2. The steps to obtain the optimal u_2 using random search algorithm are: step 1) Set an initial value for $u_2^{(0)}$ between λ_{34} and σ_{34}, step 2) In the i^{th} iteration, generate a γ_i random perturbation then update $u_2^{(i)} = u_2^{(i-1)} + \gamma_i$ with assuring that $u_2^{(i)}$ must be in the range $\sigma_{34} \leq u_2^{(i)} \leq \lambda_{34}$, then find $\bar{\mathbf{w}} = \mathbf{v}_{max}(\bar{\mathbf{A}}_2^{-1}(u_2^{(i)}\bar{\mathbf{A}}_1 + u_2^{(i)}\beta_1\bar{\mathbf{A}}_3 - \beta_1(u_2^{(i)})^2\bar{\mathbf{A}}_4)$, after that check if the objective function $\frac{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_2\bar{\mathbf{w}}}.\frac{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_3\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_4\bar{\mathbf{w}}}$ is improved, otherwise $u_2^{(i)} = u_2^{(i-1)}$. Step 3) Repeat step 2) until the function $\frac{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_1\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_2\bar{\mathbf{w}}}.\frac{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_3\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\bar{\mathbf{A}}_4\bar{\mathbf{w}}}$ does not improve anymore or a certain number of iterations is implemented.

Then, the optimal beamforming vector can be obtained using the following

equation

$$\mathbf{w} = \sqrt{P_r}\mathbf{T}^{-0.5}\bar{\mathbf{w}} \tag{3.25}$$

3.3 Simulation Results

Here, the proposed physical layer security algorithms are evaluated. In our simulation, we generate all the channels randomly as independent complex Gaussian random variables with zero mean and unit variance. All SDPs are solved efficiently using interior point method provided by Matlab CVX toolbox [3]. We obtain the results by averaging over 2000 Monte Carlo channel realization.

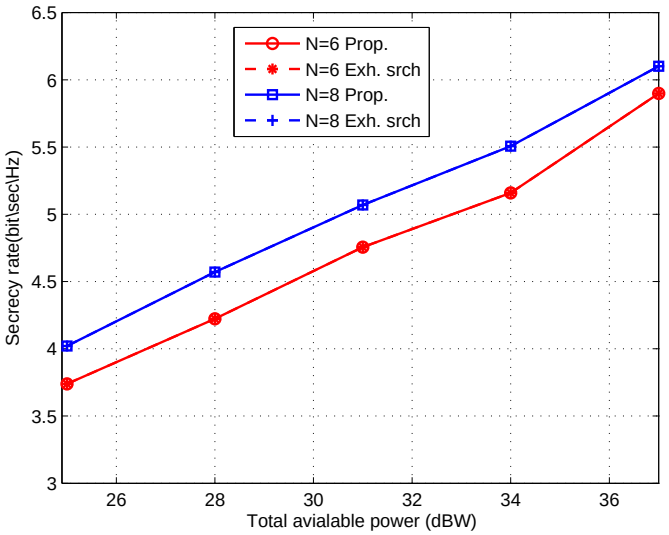

Figure 3.1: The comparison of the proposed Algorithm 3.3 and Algorithm 3.1 with various number of relays.

In Fig. 3.1, we show the comparison between the proposed Algorithm 3.3 and the exhaustive search algorithm (Algorithm 3.1) in terms of secrecy rate against the total available power when $N = 6$ and $N = 4$. For different values of the

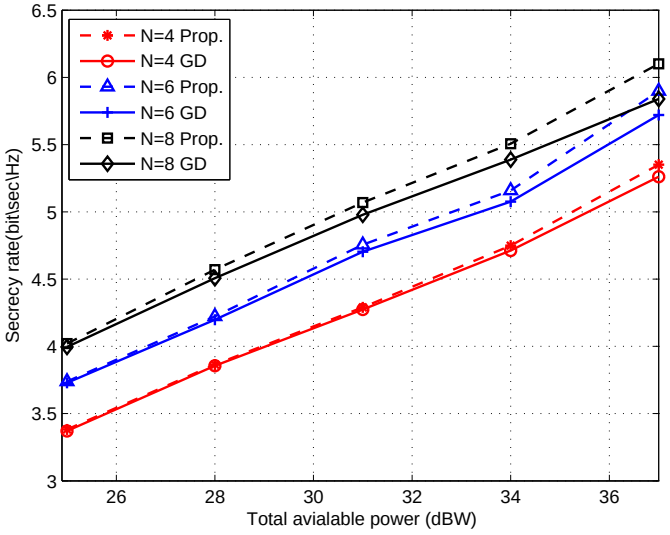

Figure 3.2: Comparison of the proposed Algorithm 3.3 and the Gradient descent method.

total available power and various number of relays, It is shown that the proposed Algorithm 3.3 provides the exact secrecy sum rate as exhaustive search grants which means that Algorithm 3.3 provides the optimal null space beamforming vector. In the exhaustive search, we perform 300 SDP to find the optimal solution per one realization.

In Fig. 3.2, we compare our optimal solution for the beamforming vector and the gradient decent method. As known, the gradient decent method does not guarantee the global optimal solution if the function has more than one local optimal solutions. Therefore, Fig. 3.2 confirms that Algorithm 3.3 provides the global optimal solution. In Fig. 3.3, the proposed optimal solution for beamforming vector (Algorithm 3.3) and the null space beamforming approach are compared in terms of secrecy rate versus the total available power. It is shown that there is no significant improvement in secrecy rate especially when the number of relays

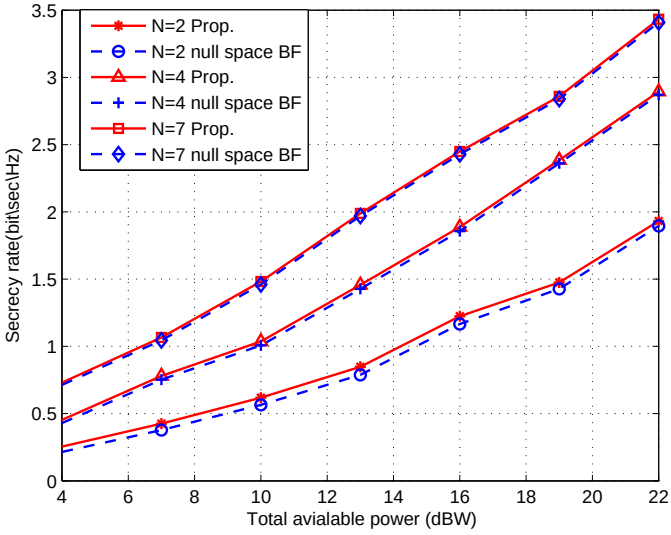

Figure 3.3: Comparison of the proposed Algorithm 3.3 and null space beamforming solution

is large. This is because that null space beamforming uses only one dimension to completely eliminate the information signal at the eavesdropper while uses the rest to maximize the destination's information rate which is fair enough.

3.4 Conclusion

In this chapter, the secrecy rate under total power constraint was maximized. The problem was expressed as a product of two RQs. Then it was convert from a nonconvex problem to a convex one with one dimensional search. After that, an efficient algorithm that guarantees the global optimal solution was proposed. Compared to the null space beamforming, we showed that the optimal beamforming vector just provides a slight improvement for the secure communication particularly when the number of relays is large.

Numerical results show that the optimal solution of maximizing the secrecy rate is not that far from the null space beamforming approach.

CHAPTER 4

IMPROVING THE PHYSICAL LAYER SECURITY IN TWRS

4.1 Introduction

In this chapter, we investigate the physical layer security in TWRS. In [10] and [11], authors studied the physical layer security in TWRS in the existence of multiple distributed relays and one eavesdropper. The secrecy sum rate has been suggested as a metric to check the performance of the system for secure communication. The problem of TWRS with multiple relays is formulated as a product of triple RQs which is hard to solve. A suboptimal solution has been proposed where the beamforming vector designed to cancel the information signals at the eavesdropper in the second phase. However, the information signals cannot be eliminated perfectly at eavesdropper since he can obtain a version of the signal directly from the transmitters in the first phase. Mathematically, the aim of this

suboptimal solution is that the optimization problem of the beamforming vector can be reduced to a product of two RQs.

In this chapter, considering the mixed signal received by the eavesdropper from the first and second phase, we obtain the optimal solution of the channel null space beamforming and the sources power for physical layer security in bidirectional transmission. Our work is distinct from the work of [10] and [11] by that, 1) we find the optimal beamforming vector (not suboptimal as given in [11]) when the sources powers are given, 2) we consider the sources powers of the two phases in the formulated optimization problem (unlike the solution given by [10]). The optimization problem is formulated as maximizing the secrecy sum rate with total power constraint. Then an iterative algorithm that finds both the beamforming vector and the sources powers is proposed. For the beamforming vector, we convert the non-convex product of two RQs to a convex problem with one dimensional search using semidefinite programming (SDP). Then we significantly simplify the problem using the generalized eigenvalues. While for the sources powers, when the beamforming vector is given, the problem has been solved using Newton's algorithm. In addition, another suboptimal approach to maximize the secrecy sum rate beside the optimal null space beamforming is proposed. This approach outperforms the null space beamforming approach especially when the number of relays is small. In our suboptimal solution, we simplify the problem by ignoring one RQ out of three that has least impact on the whole function. This solution provides a significant improvement in secrecy sum rate. In the numerical results,

we demonstrate that the proposed algorithms provide better secrecy sum rate than the previous work with different number of relays and different amount of available power.

The rest of this chapter is organized as follows; the system model is discussed in Section 4.2. In Section 4.3, we present the achievable secrecy sum rate, the problem formulation, and proposed solutions. Simulation results are presented in Section 4.4, and finally the chapter is concluded in Section 4.5.

4.2 System Model

The bidirectional communication system under consideration consists of a pair of transceivers S_1 and S_2, one eavesdropper E, and N cooperative trusted relays denoted as R_i, for $i \in \{1, 2, ..., N\}$. each node in the system has only a single antenna and working under half duplex constraint. The system is investigated under the assumption that the global CSI of all nodes even the eavesdropper is known. As shown in Fig. 4.1, there is a direct channel between both transceivers and the eavesdropper. The codewords at the transceivers are assumed to be Gaussian. We assume that each channel is a block fading channel that changes from one block to another according to a Rayleigh distribution. We denote by $\mathbf{h}_1$, $\mathbf{h}_2$ the complex channel gain between the transceivers S_1 and S_2, and the relays, respectively, by f_1, f_2 the complex channel gain between the transceivers S_1 and S_2, and E, respectively, and by $\mathbf{c}$ the complex channel gain vector between the relays and eavesdropper. We assume that there is no direct channel between the

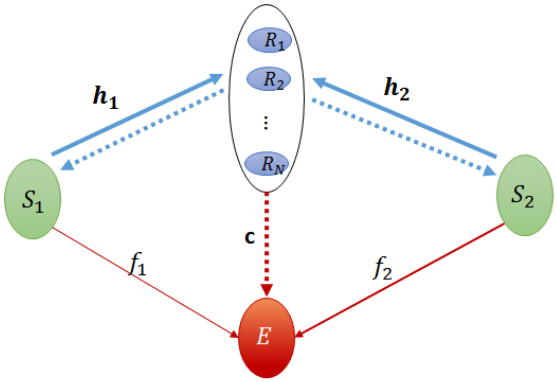

Figure 4.1: System model

transceivers. In amplify and forward scheme, the transmission of the signal takes two phases, in the first phase, both transceivers broadcast their signals to the cooperative relays. The received signal at the relays can be expressed as follows:

$$\mathbf{y}_R = \sqrt{P_1}\mathbf{h}_1 x_1 + \sqrt{P_2}\mathbf{h}_2 x_2 + \mathbf{n}_R, \tag{4.1}$$

where $\mathbf{y}_R \in R^N$ is the received vector at the relays, P_1 and P_2 are the transmission power of the transceivers S_1, S_2 respectively, x_1, x_2 are the symbols with unit power transmitted by the transceivers S_1 and S_2, respectively, and $\mathbf{n}_R$ is the complex additive white Gaussian noise vector at the relays with covariance matrix $\sigma_R^2\mathbf{I_N}$. On the other hand, the received signal at the eavesdropper in the first phase can be written as:

$$y_E^{(1)} = \sqrt{P_1} f_1 x_1 + \sqrt{P_2} f_2 x_2 + n_{e1}, \tag{4.2}$$

where n_{e1} is the additive noise at the eavesdropper with variance σ_{e1}^2. In the second phase, relays multiply the information signal by a complex vector $\mathbf{w}$. Therefore,

we can express the transmitted signal at the relays as:

$$\mathbf{x}_R = \mathbf{W}\mathbf{y}_R, \tag{4.3}$$

where $\mathbf{y}_R$ is given by (4.1), and $\mathbf{W}$ is a diagonal matrix that contains the complex weight vector of the relays $\mathbf{W} = diag(\mathbf{w})$. The received signals at the transceivers can be written as:

$$y_{S1} = \sqrt{P_2}\mathbf{w}^H\mathbf{a}_{12}x_2 + \sqrt{P_1}\mathbf{w}^H\mathbf{a}_{11}x_1 + \mathbf{w}^H\mathbf{H}_1\mathbf{n}_R + n_{S1}, \tag{4.4}$$

$$y_{S2} = \sqrt{P_1}\mathbf{w}^H\mathbf{a}_{12}x_1 + \sqrt{P_2}\mathbf{w}^H\mathbf{a}_{22}x_2 + \mathbf{w}^H\mathbf{H}_2\mathbf{n}_R + n_{S2}, \tag{4.5}$$

where $\mathbf{H}_1 = diag(\mathbf{h}_1)$, $\mathbf{H}_2 = diag(\mathbf{h}_2)$, $\mathbf{a}_{12}$=$\mathbf{H}_1^H\mathbf{h}_2$, $\mathbf{a}_{11} = \mathbf{H}_1^H\mathbf{h}_1$, $\mathbf{a}_{22} = \mathbf{H}_2^H\mathbf{h}_2$, and n_{S_1}, n_{S_2} are the additive zero mean noises with σ_1^2, σ_2^2 at S_1, S_2, respectively.

The terms $\sqrt{P_1}\mathbf{w}^H\mathbf{a}_{11}x_1$ in equation (5.2) and $\sqrt{P_2}\mathbf{w}^H\mathbf{a}_{22}x_2$ in equation (5.3) are called the backward self-interference, and can be eliminated if each transmitter knows its instantaneous channel and the beamforming vector $\mathbf{w}$. Equations (5.2) and (5.3) can be expressed as follows:

$$y_{S1} = \sqrt{P_2}\mathbf{w}^H\mathbf{a}_{12}x_2 + \mathbf{w}^H\mathbf{H}_1\mathbf{n}_R + n_{S1}, \tag{4.6}$$

$$y_{S2} = \sqrt{P_1}\mathbf{w}^H\mathbf{a}_{12}x_1 + \mathbf{w}^H\mathbf{H}_2\mathbf{n}_R + n_{S2}, \tag{4.7}$$

while the received signal at the eavesdropper in the second phase is

$$y_E^{(2)} = \sqrt{P_2}\mathbf{w}^H\mathbf{a}_{c2}x_2 + \sqrt{P_1}\mathbf{w}^H\mathbf{a}_{c1}x_1 + \mathbf{w}^H\mathbf{C}\mathbf{n}_R + n_{e2}, \tag{4.8}$$

where $\mathbf{C} = diag(\mathbf{c})$, $\mathbf{a}_{c2}$=$\mathbf{C}^H\mathbf{h}_2$, $\mathbf{a}_{c1} = \mathbf{C}^H\mathbf{h}_1$, and n_{e2} is the additive zero mean noise with variance σ_{e2}^2 at eavesdropper in the second phase. Since the eavesdropper has two chances to get the information signal from the first and second phase, it can use maximum ratio combining to maximize its SNR and create an equivalent MIMO system. The received signal at the eavesdropper is

$$\mathbf{y}_E = \mathbf{E}\mathbf{x} + \mathbf{n}_e, \tag{4.9}$$

where $\mathbf{y}_E = \begin{bmatrix} y_E^{(1)} \\ y_E^{(2)} \end{bmatrix}$, $\mathbf{E} = \begin{bmatrix} \sqrt{P_1}f_1 & \sqrt{P_2}f_2 \\ \sqrt{P_1}\mathbf{w}^H\mathbf{a}_{c1} & \sqrt{P_2}\mathbf{w}^H\mathbf{a}_{c2} \end{bmatrix}$, $\mathbf{n}_e = \begin{bmatrix} n_{e1} \\ \mathbf{w}^H\mathbf{C}\mathbf{n}_R + n_{e2} \end{bmatrix}$, and $\mathbf{s} = \begin{bmatrix} s_1 & s_2 \end{bmatrix}$.

Similar to the information rates given in OWRS, in TWRS, the information rate at the transceivers can be written as:

$$R_{S_1} = \frac{1}{2}\log(1 + \frac{P_2\mathbf{w}^H\mathbf{R}_{12}\mathbf{w}}{\sigma_1^2 + \mathbf{w}^H\sigma_R^2\mathbf{R}_{11}\mathbf{w}}), \tag{4.10a}$$

$$R_{S_2} = \frac{1}{2}\log(1 + \frac{P_1\mathbf{w}^H\mathbf{R}_{12}\mathbf{w}}{\sigma_2^2 + \mathbf{w}^H\sigma_R^2\mathbf{R}_{22}\mathbf{w}}), \tag{4.10b}$$

where $\mathbf{R}_{12} = \mathbf{a}_{12}\mathbf{a}_{12}^H$, $\mathbf{R}_{11} = \mathbf{H}_1\mathbf{H}_1^H$, $\mathbf{R}_{22} = \mathbf{H}_2\mathbf{H}_2^H$. The information rate at

eavesdropper is

$$R_E = \frac{1}{2}\log\det\,(\mathbf{I} + \mathbf{E}\mathbf{E}^H\mathbf{N}_e^{-1}), \tag{4.11}$$

where $\mathbf{N}_e$ is the covariance matrix of the received noise at eavesdropper which is:

$$\mathbf{N}_e = \begin{bmatrix} \sigma_{e1}^2 & 0 \\ 0 & \sigma_{e2}^2 + \mathbf{w}^H\sigma_R^2\mathbf{R}_{cc}\mathbf{w} \end{bmatrix}. \tag{4.12}$$

4.3 Problem Formulation

In this section, we aim to look for the optimal weight vector to maximize the secrecy sum rate while maintaining the total transmit power below a given maximum value. The secrecy sum rate is expressed as follows:

$$\begin{aligned} R_S^{sum} = &\frac{1}{2}\log(1 + \frac{P_2\mathbf{w}^H\mathbf{R}_{12}\mathbf{w}}{\sigma_1^2 + \sigma_R^2\mathbf{w}^H\mathbf{R}_{11}\mathbf{w}}) \\ &+\frac{1}{2}\log(1 + \frac{P_1\mathbf{w}^H\mathbf{R}_{12}\mathbf{w}}{\sigma_2^2 + \sigma_R^2\mathbf{w}^H\mathbf{R}_{22}\mathbf{w}}) \\ &-\frac{1}{2}\log\det\,(\mathbf{I} + \mathbf{E}\mathbf{E}^H\mathbf{N}_e^{-1}). \end{aligned} \tag{4.13}$$

Therefore, the optimization problem can be expressed as

$$\max_{\mathbf{w}} \qquad R_S^{sum} \tag{4.14a}$$

$$s.t \qquad P_1 + P_2 + \mathbf{w^H D w} \leq P_T, \tag{4.14b}$$

where $\mathbf{D}$ is a diagonal positive definite matrix $\mathbf{D} = P_1 R_{11} + P_2 R_{22} + \sigma_R^2 \mathbf{I}$, and P_T is the total available maximum power at relays and transceivers. It was in [10] that Problem (4.14) can be written as:

$$\max_{\mathbf{w}} \quad \frac{\mathbf{w}^H \mathbf{C}_1 \mathbf{w}}{\mathbf{w}^H \mathbf{C}_2 \mathbf{w}} . \frac{\mathbf{w}^H \mathbf{C}_3 \mathbf{w}}{\mathbf{w}^H \mathbf{C}_4 \mathbf{w}} . \frac{\mathbf{w}^H \mathbf{C}_5 \mathbf{w}}{\mathbf{w}^H \mathbf{C}_6 \mathbf{w}}, \tag{4.15}$$

where

$$\mathbf{C}_1 = P_2 \mathbf{R}_{12} + \sigma_R^2 \mathbf{R}_{11} + P_r^{-1} \sigma_1^2 \mathbf{D},$$

$$\mathbf{C}_2 = \sigma_R^2 \mathbf{R}_{11} + \sigma_1^2 P_r^{-1} \mathbf{D},$$

$$\mathbf{C}_3 = P_1 \mathbf{R}_{12} + \sigma_R^2 \mathbf{R}_{22} + \sigma_2^2 P_r^{-1} \mathbf{D},$$

$$\mathbf{C}_4 = \sigma_R^2 \mathbf{R}_{22} + \sigma_2^2 P_r^{-1} \mathbf{D},$$

$$\mathbf{C}_5 = \sigma_{e2}^2 \sigma_R^2 \mathbf{R}_{cc} + \sigma_{e2}^2 \sigma_{e1}^2 P_r^{-1} \mathbf{D},$$

$$\mathbf{C}_6 = (P_1 P_2 |f_2|^2 + \sigma_{e1}^2 P_1) \mathbf{R}_{c1} + (P_1 P_2 |f_1|^2 + \sigma_{e1}^2 P_2) \mathbf{R}_{c2}$$

$$+ (P_1 \sigma_R^2 |f_2|^2 + P_2 \sigma_R^2 |f_1|^2 + \sigma_R^2 \sigma_e^2) \mathbf{R}_{cc} + (P_1 \sigma_{e2}^2 |f_2|^2 +$$

$$P_2 \sigma_{e2}^2 |f_1|^2 + \sigma_{e1}^2 \sigma_{e2}^2) P_r^{-1} \mathbf{D}$$

where P_r is the summation of the relays' total transmit power, $\mathbf{R}_{c1} = \mathbf{a}_{c1} \mathbf{a}_{c1}^H$, $\mathbf{R}_{c2} = \mathbf{a}_{c2} \mathbf{a}_{c2}^H$, $\mathbf{R}_{cc} = \mathbf{C}\mathbf{C}^H$, and $\mathbf{R}_{22} = \mathbf{H}_2 \mathbf{H}_2^H$. We can obtain $P_r = E\{\mathbf{y}_R^H \mathbf{y}_R\} = \mathbf{w}^H \mathbf{D} \mathbf{w}$. Problem (4.15) is a product of triple RQs, that is generally considered as a difficult problem. Here, we propose two suboptimal solutions for maximizing the secrecy sum rate when the total power is constrained with a certain value.

4.3.1 Null Space Beamforming

In this section, after we design the relays weight to be nulled at the eavesdropper, we maximize the secrecy sum rate when the total power of relays and transceivers are constrained with a predefined value. In other words, we design $\mathbf{w}$ to be orthogonal with the vectors a_{c1}, a_{c2} to guarantee that the rate of eavesdropper coming from the second phase is zero. Let $\mathbf{G}$ be the equivalent channel matrix $G = [\mathbf{a}_{c1}\ \mathbf{a}_{c2}]$, hence $\mathbf{G}^H\mathbf{w} = 0$. According to this case, eavesdropper cannot obtain any information from the second phase since the signal forwarded from relays completely nulled out at the eavesdropper. Therefore, the eavesdropper can receive only one version of transmitted signals coming from the first phase. The rate of the eavesdropper can be expressed as:

$$R_e = 0.5\log(1 + (P_1|f_1|^2 + P_2|f_2|^2)/\sigma_{e1}^2).$$

Thus, the secrecy sum rate can be written as:

$$\begin{aligned} R_S^{sum} = &\frac{1}{2}\log(1 + \frac{P_2\mathbf{w}^H\mathbf{R}_{12}\mathbf{w}}{\sigma_1^2 + \sigma_R^2\mathbf{w}^H\mathbf{R}_{11}\mathbf{w}}) \\ &+\frac{1}{2}\log(1 + \frac{P_1\mathbf{w}^H\mathbf{R}_{12}\mathbf{w}}{\sigma_2^2 + \sigma_R^2\mathbf{w}^H\mathbf{R}_{22}\mathbf{w}}) \\ &-\frac{1}{2}\log(1 + (P_1|f_1^2| + P_2|f_2^2|)/\sigma_{e1}^2). \end{aligned} \tag{4.16}$$

We rewrite $\mathbf{w}$ as $\mathbf{w} = \mathbf{Zq}$ where $\mathbf{Z}$ is the projection matrix into the null space of $\mathbf{G}$, and $\mathbf{q}$ can be any vector $(1 \times (N-2))$ The optimization problem can be

reformulated as:

$$\max_{\mathbf{q},P_1,P_2} \quad \frac{(1+\frac{P_1\mathbf{q}^H\mathbf{Z}\mathbf{R}_{12}\mathbf{Z}\mathbf{q}}{\sigma_1^2+\sigma_R^2\mathbf{q}^H\mathbf{Z}\mathbf{R}_{22}Z\mathbf{q}})(1+\frac{P_2\mathbf{q}^H\mathbf{Z}\mathbf{R}_{12}\mathbf{Z}\mathbf{q}}{\sigma_2^2+\sigma_R^2\mathbf{q}^HZ\mathbf{R}_{11}\mathbf{Z}\mathbf{q}})}{(1+(P_1|f_1|^2+P_2|f_2|^2)/\sigma_{e1}^2)} \tag{4.17a}$$

$$s.t. \qquad \mathbf{q}\mathbf{Z}^H\mathbf{D}\mathbf{Z}\mathbf{q} \leq P_T - P_1 - P_2. \tag{4.17b}$$

Problem (4.17) is not that easy to solve for both the optimal beamforming vector and sources powers. Thus, we adopt an iterative algorithm that obtains $\mathbf{q}$ and P_1, P_2 alternatively.

Optimizing the beamforming vector

In this subsection, we will obtain the optimal beamforming vector that eliminate the information signal at eavesdropper when the powers of the sources are fixed. In [11], it is proved that the constraint (4.17b) holds with equality at optimality. Let $P_r = P_T - P_1 - P_2$ and $\mathbf{B} = \frac{1}{P_r}\mathbf{Z}^\mathbf{H}\mathbf{D}\mathbf{Z}$. Therefore, $\mathbf{q}^H\mathbf{B}\mathbf{q} = 1$. Let's denote the unit norm complex vector $\bar{\mathbf{q}}$ such that $\mathbf{B}^{0.5}\mathbf{q} = \bar{\mathbf{q}}$, then $\bar{\mathbf{q}}^H\bar{\mathbf{q}} = \mathbf{q}^H\mathbf{B}\mathbf{q} = 1$. Therefore, optimization problem (4.17) is equivalent to the following

$$\max_{\mathbf{q}} \qquad \frac{\bar{\mathbf{q}}^H\bar{\mathbf{C}}_1\bar{\mathbf{q}}}{\bar{\mathbf{q}}^H\bar{\mathbf{C}}_2\bar{\mathbf{q}}}.\frac{\bar{\mathbf{q}}^H\bar{\mathbf{C}}_3\bar{\mathbf{q}}}{\bar{\mathbf{q}}^H\bar{\mathbf{C}}_4\bar{\mathbf{q}}} \tag{4.18a}$$

$$s.t \qquad \|\bar{\mathbf{q}}\|^2 = 1, \tag{4.18b}$$

where

$$\bar{\mathbf{C}}_1 = \frac{\sigma_1^2\mathbf{I}}{P_r} + \sigma_R^2\mathbf{B}^{-0.5}\mathbf{Z}^H\mathbf{R}_{11}\mathbf{Z}\mathbf{B}^{-0.5} + P_2\mathbf{B}^{-0.5}\mathbf{Z}^H\mathbf{R}_{12}\mathbf{Z}\mathbf{B}^{-0.5},$$

$$\bar{\mathbf{C}}_2 = (1 + (P_1|f_1|^2 + P_2|f_2|^2)/\sigma_{e1}^2)(\frac{\sigma_1^2\mathbf{I}}{P_r} + \sigma_R^2\mathbf{B}^{-0.5}\mathbf{Z}^H\mathbf{R}_{11}\mathbf{Z}\mathbf{B}^{-0.5}),$$

$$\bar{\mathbf{C}}_3 = \frac{\sigma_2^2\mathbf{I}}{P_r} + \sigma_R^2\mathbf{B}^{-0.5}\mathbf{Z}^H\mathbf{R}_{22}\mathbf{Z}\mathbf{B}^{-0.5} + P_1\mathbf{B}^{-0.5}\mathbf{Z}^H\mathbf{R}_{12}\mathbf{Z}\mathbf{B}^{-0.5},$$

$$\bar{\mathbf{C}}_4 = \frac{\sigma_2^2\mathbf{I}}{P_r} + \sigma_R^2\mathbf{B}^{-0.5}\mathbf{Z}^H\mathbf{R}_{22}\mathbf{Z}\mathbf{B}^{-0.5}.$$

Problem (4.18) is similar to the Problem (3.5) investigated in chapter 3. Therefore, we solve Problem (4.18) by going with the same procedures used in solving (3.5). Hence, Algorithm 3.3 can be used to provide the optimal solution of Problem (4.18).

Optimizing the transceivers power

In this part, we obtain the optimal sources power when the beamforming vector is given. Problem (4.17) can be reformulated as follows:

$$\max_{P_1,P_2} \frac{(1 + P_2y_1)(1 + P_1y_2)}{(1 + (P_1|f_1|^2 + P_2|f_2|^2)/\sigma_{e1}^2)} \tag{4.19a}$$

$$s.t \quad P_1k_1 + P_2k_2 \geq P_T - \sigma_R^2\mathbf{w}^H\mathbf{w}, \tag{4.19b}$$

where $y_1 = \frac{{}_2\mathbf{w}^H\mathbf{R}_{12}\mathbf{w}}{\sigma_1^2+\sigma_R^2\mathbf{w}^H\mathbf{R}_{11}\mathbf{w}}$, $y_2 = \frac{\mathbf{w}^H\mathbf{R}_{12}\mathbf{w}}{\sigma_2^2+\sigma_R^2\mathbf{w}^H\mathbf{R}_{22}\mathbf{w}}$, $k_1 = 1 + \mathbf{w}^H R_{11}\mathbf{w}$ and $k_2 = 1 + \mathbf{w}^H R_{22}\mathbf{w}$. It is shown earlier that at optimality the inequality in (4.19b) must be satisfied with equality. Hence, we can substitute $P_2 = \frac{P_T-\sigma_R^2\mathbf{w}^H\mathbf{w}-P_1k_1}{k_2}$ in the objective function (4.19a) to have the optimization problem as follows:

$$\max_{P_1} \frac{a_0 + P_1a_1 + P_1^2a_2}{b_0 + P_1b_1}, \tag{4.20}$$

where $a_0 = 1 + \frac{y_1P_T}{k_2} - \frac{y_1\sigma^2\bar{\mathbf{q}}^H\bar{\mathbf{q}}}{k_2}$, $a_1 = y_1 - \frac{y_1k_1}{k_2} + \frac{y_1y_2P_T}{k_2} - \frac{y_1y_2\bar{\mathbf{q}}^H\bar{\mathbf{q}}}{k_2}$, $a_2 = y_2 - \frac{y_1k_1}{k_2}$, $b_1 = \frac{1}{\sigma^2}(|f_e|^2 - \frac{k_1}{\sigma^2k_2}|g_e|^2)$, and $b_0 = 1 + \frac{P_T-\sigma^2\bar{\mathbf{q}}^H\bar{\mathbf{q}}}{k_2}|g_e|^2$.

Problem (4.20) was considered in [11] and it was solved using Newton's algorithm to obtain the optimal sources powers when the beamforming vector is given. Therefore, we provide Algorithm 4.1 to obtain both the beamforming vector and the sources power.

Algorithm 4.1 Finding the joint $(P_1^*, P_2^*, \mathbf{w}^*)$

1. Give P_1 and P_2 initial values.
2. Use Algorithm 3.3 to find the optimal null space beamforming vector $\mathbf{w}$.
3. Use Newton algorithm to solve Problem (4.20) to obtain P_1 and P_2.
4. Repeat steps 2) and 3) until $(P_1, P_2, \mathbf{w})$ converge.

It is easy to prove that Algorithm 4.1 is convergent since as the number of iterations increases the objective function of Problem (4.17) will increase. In addition, the objective function is bounded above because of that the total available power is bounded above. On the other hand, Algorithm 4.1 cannot guarantee the joint global optimal solution because the original function (4.17) is not convex.

Therefore, to guarantee a near global optimal solution, we should give the initial values for P_1 and P_2 close to their global optimal solution. Authors of [10] provided the joint optimal solution but with ignoring the signal coming from the first phase (i.e., the expression $(1 + (P_1|f_1|^2 + P_2|f_2|^2)/\sigma_{e1}^2)$ has not been included in the optimization problem). Accordingly, we can use the solution provided in [10] as an initial values for P_1 and P_2 then implement Algorithm 4.1.

4.3.2 Suboptimal Solution: Ignoring one Rayleigh quotient (IORQ)

In this section, we focus on optimizing the beamforming vector without considering the sources powers. The disadvantage of the null space beamforming approach is that it is inefficient solution in case of the number of relays is small since the weight vector has to be orthogonal with two vectors which means that the available dimensions to beamform the information signal for sources are only $N - 2$ dimensions. Besides, it is not applicable when $N < 3$. It is crucial to observe that eliminating the information signal at the eavesdropper degrades the information rate at the transceivers; i.e., there is a trade off between the transceivers information rates and the information rate at the eavesdropper. On the other hand, as the number of relays increases (goes to infinity), the optimal null space beamforming approach will approach the optimal solution of Problem (4.15). It can be demonstrated that as the number of relays increases the information rates at the transceivers will increase and the information rate at eavesdropper will go to zero

which is equivalent to the optimal null space beamforming approach. Therefore, In the following approach, we deal directly with the original problem (4.15) to maximize the whole secrecy sum rate aiming to enhance the secrecy sum rate especially when number of relays is small. We have $\mathbf{C}_2, \mathbf{C}_3$ and $\mathbf{C}_5$ are diagonal matrices and are a partial of the other matrices which indicates that they have less impact on the whole function than the other matrices. Thus, our approach based on ignoring one Rayleigh quotient either $\frac{\mathbf{w}^H\mathbf{C}_5\mathbf{w}}{\mathbf{w}^H\mathbf{C}_2\mathbf{w}}$ or $\frac{\mathbf{w}^H\mathbf{C}_5\mathbf{w}}{\mathbf{w}^H\mathbf{C}_4\mathbf{w}}$ and solve the rest of the function. Therefore, the problem can be written in two ways:

$$\max_{\mathbf{w}} \quad \frac{\mathbf{w}^H\mathbf{C}_1\mathbf{w}}{\mathbf{w}^H\mathbf{C}_2\mathbf{w}}.\frac{\mathbf{w}^H\mathbf{C}_3\mathbf{w}}{\mathbf{w}^H\mathbf{C}_6\mathbf{w}}, \tag{4.21a}$$

or

$$\max_{\mathbf{w}} \quad \frac{\mathbf{w}^H\mathbf{C}_1\mathbf{w}}{\mathbf{w}^H\mathbf{C}_4\mathbf{w}}.\frac{\mathbf{w}^H\mathbf{C}_3\mathbf{w}}{\mathbf{w}^H\mathbf{C}_6\mathbf{w}}. \tag{4.22a}$$

Algorithm 3.3 can be used to solve both Problems (4.21) and (4.22) and select the solution vector that maximize the objective function in (4.15) more than the other. But this way will double the complexity of the problem by implementing Algorithm 3.3 twice. Instead, We propose another method to decide whether to solve (4.21) or (4.22). It is known that the objective function in (4.15) is bounded

by

$$\begin{aligned}\frac{\mathbf{w}^H\mathbf{C_1}\mathbf{w}}{\mathbf{w}^H\mathbf{C_4}\mathbf{w}}.\frac{\mathbf{w}^H\mathbf{C_3}\mathbf{w}}{\mathbf{w}^H\mathbf{C_6}\mathbf{w}}\lambda_{min}(\mathbf{C_2^{-1}C_5}) &\leq \frac{\mathbf{w}^H\mathbf{C_1}\mathbf{w}}{\mathbf{w}^H\mathbf{C_2}\mathbf{w}}.\frac{\mathbf{w}^H\mathbf{C_3}\mathbf{w}}{\mathbf{w}^H\mathbf{C_4}\mathbf{w}}.\frac{\mathbf{w}^H\mathbf{C_5}\mathbf{w}}{\mathbf{w}^H\mathbf{C_6}\mathbf{w}} \\ &\leq \frac{\mathbf{w}^H\mathbf{C_1}\mathbf{w}}{\mathbf{w}^H\mathbf{C_4}\mathbf{w}}.\frac{\mathbf{w}^H\mathbf{C_3}\mathbf{w}}{\mathbf{w}^H\mathbf{C_6}\mathbf{w}}\lambda_{max}(\mathbf{C_2^{-1}C_5})\end{aligned} \tag{4.23}$$

It is clear that solving (4.22) provides the optimal solution if $\lambda_{max}(\mathbf{C_2^{-1}C_5}) = \lambda_{min}(\mathbf{C_2^{-1}C_5})$ and it is near the optimal solution (or ϵ-optimal) if $\frac{\lambda_{max}(\mathbf{C_2^{-1}C_5})}{\lambda_{min}(\mathbf{C_2^{-1}C_5})} \leq 1+\epsilon$, where ϵ is small value. Similarly,

$$\begin{aligned}\frac{\mathbf{w}^H\mathbf{C_1}\mathbf{w}}{\mathbf{w}^H\mathbf{C_2}\mathbf{w}}.\frac{\mathbf{w}^H\mathbf{C_3}\mathbf{w}}{\mathbf{w}^H\mathbf{C_6}\mathbf{w}}\lambda_{min}(\mathbf{C_4^{-1}C_5}) &\leq \frac{\mathbf{w}^H\mathbf{C_1}\mathbf{w}}{\mathbf{w}^H\mathbf{C_2}\mathbf{w}}.\frac{\mathbf{w}^H\mathbf{C_3}\mathbf{w}}{\mathbf{w}^H\mathbf{C_4}\mathbf{w}}.\frac{\mathbf{w}^H\mathbf{C_5}\mathbf{w}}{\mathbf{w}^H\mathbf{C_6}\mathbf{w}} \\ &\leq \frac{\mathbf{w}^H\mathbf{C_1}\mathbf{w}}{\mathbf{w}^H\mathbf{C_2}\mathbf{w}}.\frac{\mathbf{w}^H\mathbf{C_3}\mathbf{w}}{\mathbf{w}^H\mathbf{C_6}\mathbf{w}}\lambda_{max}(\mathbf{C_4^{-1}C_5})\end{aligned} \tag{4.24}$$

Consequently, we check that if $\frac{\lambda_{max}(\mathbf{C_2^{-1}C_5})}{\lambda_{min}(\mathbf{C_2^{-1}C_5})} \leq \frac{\lambda_{max}(\mathbf{C_4^{-1}C_5})}{\lambda_{min}(\mathbf{C_4^{-1}C_5})}$, we solve Problem (4.22), otherwise we solve (4.21) since we do not have to solve eigenvalue problems because the eigenvalues of the matrices $\mathbf{C_4^{-1}C_5}$ and $\mathbf{C_2^{-1}C_5}$ are their diagonal values. It is important to say that solving the product of two Rayleigh quotients is the first step to solve the product of three RQs and provide the optimal beamforming vector.

4.4 Simulation Results

In this part of the chapter, the simulation results are presented to demonstrate the effectiveness of the proposed physical layer security algorithms. In each simulation result, we generate the channels randomly as independent complex Gaussian

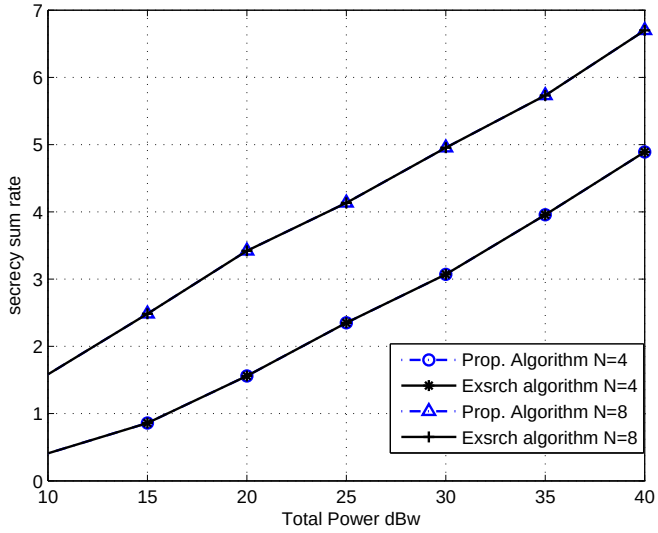

Figure 4.2: Comparison of the proposed Algorithm 3.3 and the exhaustive search (Algorithm 3.1) for null space beamforming by plotting the secrecy sum rate against the total available power with N=4, and N=8.

random variables with zero mean and unit variance. All SDP problems are solved efficiently using interior point method provided by Matlab CVX toolbox [3]. We obtain each result by averaging over 2000 Monte Carlo channel realization. In Fig. 4.2 we show the comparison between the exhaustive search (Algorithm 3.1) for u_2 implemented in Problem (3.9) and the proposed algorithm 3 in terms of secrecy sum rate against the total available maximum transmit power when N=4 and N=8. For different values of the total available power and different number of relays, It is shown that the proposed Algorithm 3.3 provides the exact secrecy sum rate as the exhaustive search grants which means that Algorithm 3.3 provides the optimal null space beamforming vector. Hence, Algorithm 3.3 can be used to solve Problem (4.18) instead of Algorithm 3.1 to avoid the complexity of implementing multiple SDP problems.

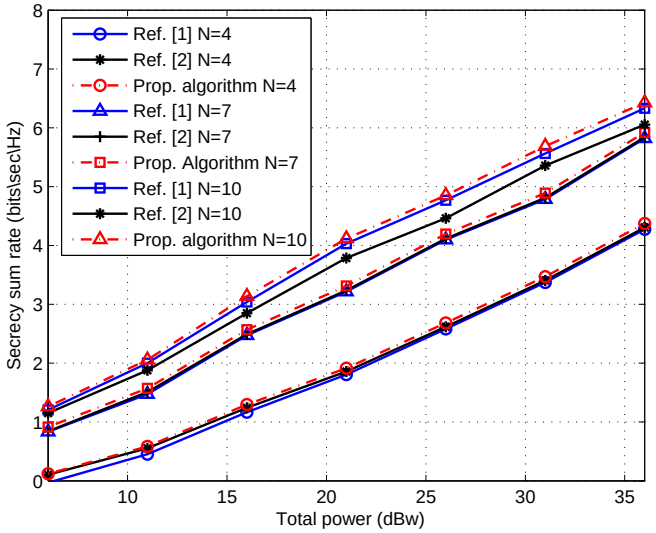

Figure 4.3: Comparison of the proposed Algorithm 3.3 for null space beamforming and the solution provided by reference [10] and [11] by plotting secrecy sum rate against the total obtainable power with different number of relays.

In Fig. 4.3, our proposed solution (Algorithm 4.1) for null space beamforming is compared to the approaches proposed in [10] and [11]. It is shown that the security improves as the total available power increases. This is because of that most of the increase in the total available power is devoted for the relays power which increases the mutual information rates at transceivers while the information rate at eavesdropper cannot improve anymore. It is also shown in Fig. 4.3 that as the number of relays increases, the secrecy sum rate increases because of the array gain that helps in increasing the information rates at the transceivers while keeping the information rate at the eavesdropper nulled. It is shown that Algorithm 4.1 provides better performance regardless of the total available power and the number of relays are. Authors of [10] did not provide a solution for the beamforming vector when the sources powers are given, while authors in [11] provided a suboptimal

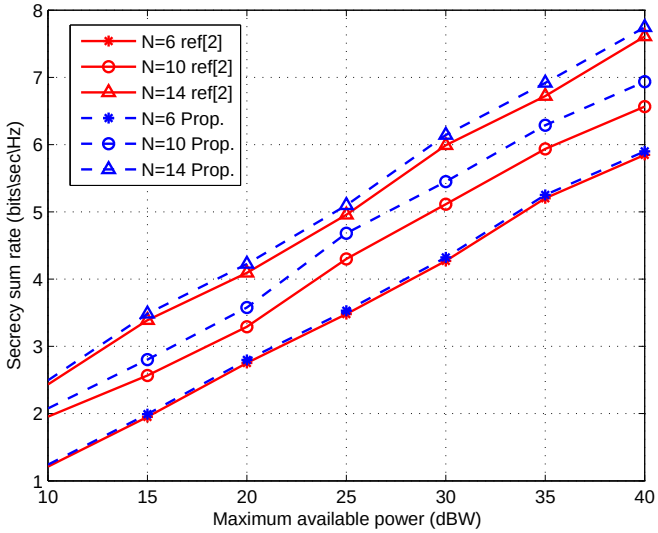

Figure 4.4: Comparison of our solution for null space beamforming and the solution provided by reference [11] by plotting secrecy sum rate against the total available power at relays with various number of relays

solution for the product of two Rayleigh quotients maximizing problem. Therefore, we compare the proposed Algorithm 3.3 that solves the product of two Rayleigh quotients and the algorithm proposed in [11] in Fig 4.4 without optimizing the sources powers. We assume that the sources powers $P_1 = P_2 = 0.25P_T$ for both algorithms. It is also shown that our solution outperforms the solution provided in [11] in all situations.

In Fig. 4.5, we demonstrate that Algorithm 3.3 grants the global optimal solution for maximizing the product of two Rayleigh quotients when the beamforming vector is not designed to be nulled at the eavesdropper; i.e., we solved our proposed approach IORQ using two algorithms: the exhaustive search and Algorithm 3.3 and it is shown that they are identical.

As shown before that the null space beamforming is not efficient when there

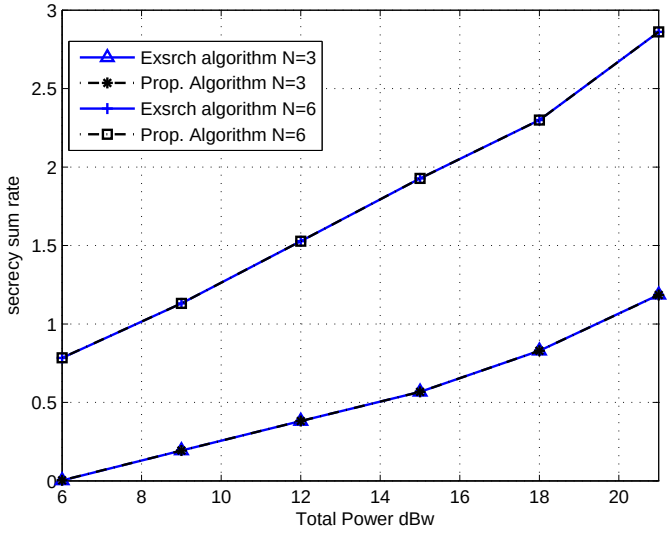

Figure 4.5: Comparison of our solution Algorithm 3.3 for the IORQ suboptimal solution and the exhaustive search by plotting the secrecy sum rate against the overall obtainable power at relays and sources with N=3, and N=6.

is a few relays. Therefore, in Fig. 4.6, we compare our proposed approach IORQ with our optimal null space beamforming in terms of the secrecy sum rate against the total available power. The comparison implemented when $P_1 = P_2 = 0.25P_T$ for both approaches. Fig. 4.6 shows that the suboptimal approach IORQ provides a substantial improvement in secrecy sum rate when N=3 and 4. In the optimal null space beamforming, it is shown that when the number of relays is 3 and in low power, the secrecy sum rate is negative which means that the information rate of the eavesdropper coming from the first phase is greater than the the summation of the information rates of the transceivers. This is due to the reason that two dimensions are used to eliminate the eavesdropper's information rate, and hence the remaining one dimension is not enough to improve the information rates at the sources. In contrast, as shown in Fig. 4.6, proposed IORQ guarantees non

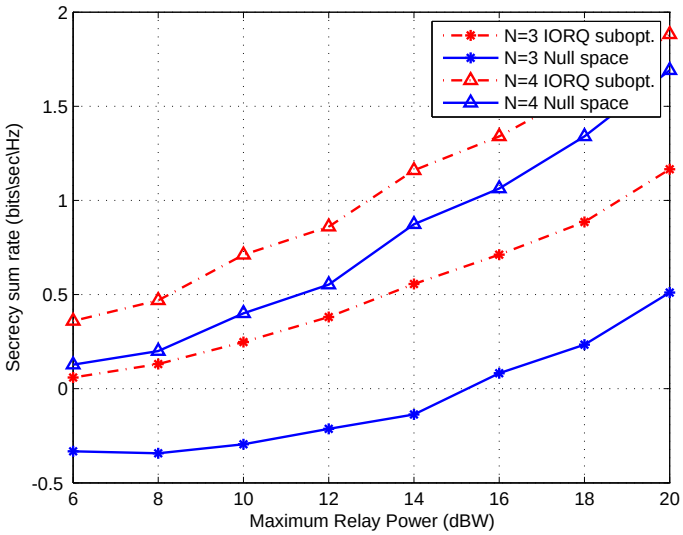

Figure 4.6: Comparison of our solution for null space beamforming and the proposed suboptimal solution (ignoring one Rayleigh quotient) by plotting secrecy sum rate against the total available power with N=3, and N=4.

zero secrecy sum rate even if the number of relays is 3 and ithe power is low.

Although the number of relays increases in Fig. 4.7, IORQ still provides a significant improvement in secure communications over that of the proposed optimal null space beamforming when $N = 5$ and $N = 6$. This shows that the impact of the ignored Rayleigh quotient on the whole function (4.15) is not that significant.

In Fig. 4.8, it is shown that the IORQ outperforms the null space beamforming when the total available power is low. This is because of the fact that the null space beamforming degrades the SNR at transceivers in order to null it at the eavesdropper. However, when the available power at the relays is high, the SNR at the transceivers will improve. In other words, increasing the power at the relays will increase the information rates at transceivers while keeping the eavesdropper's

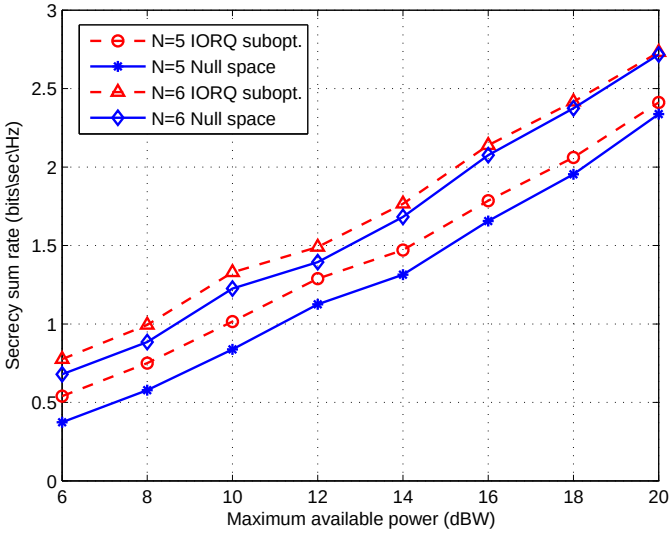

Figure 4.7: Comparison of our solution for null space beamforming and the proposed suboptimal solution (ignoring one Rayleigh quotient) by plotting secrecy sum rate against the total available power with N=5, and N=6.

rate nulled.

To show the relationship between the secrecy sum rate and the number of relays for both approaches, Fig. 4.9, shows the secrecy sum rate versus N when the total available power is 5 dBW, 10 dBW and 15 dBW. It is shown that as the number of relays increases, the difference between the performance of IORQ and the null space beamforming diminishes. This is because of the reason that the null space beamforming approaches the optimal solution of Problem (4.15) as N increases. It can also be realized from Fig. 8 that as N increases the enhancement of the secrecy sum rate per one node goes down. This is because the amount increased due to the array gain will decrease as the number of relays increases. Therefore, when N is large, it is fair to choose two dimensions to eliminate the signal at the eavesdropper and use the rest to maximize the information rates at the transceivers. It is also

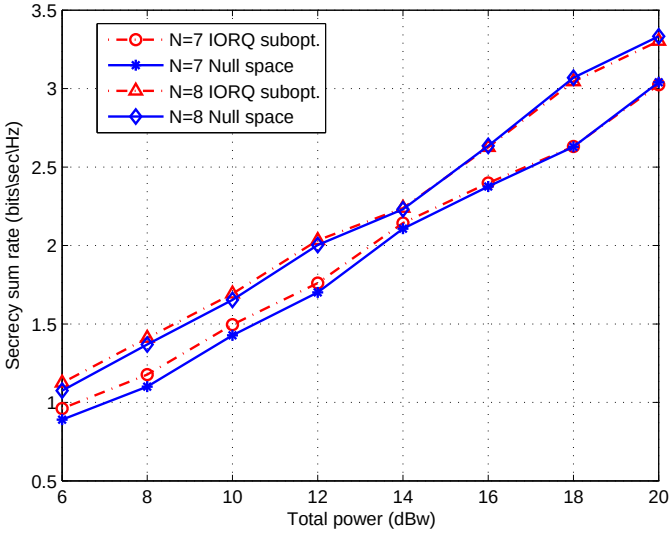

Figure 4.8: Comparison of our solution for null space beamforming and the proposed suboptimal solution (ignoring one Rayleigh quotient) by plotting secrecy sum rate against the total available power with N=7, and N=8.

shown that when the total available power is low, IORQ still outperforms the null space beamforming until $N = 10$. On the other hand, in the high power cases (e.g., $P = 15dBW$), null space beamforming starts to perform better when $N = 8$ and larger. It is clear that even with high power transmission with a large number of relays, optimal null space beamforming provides a very slight improvement in secure communication better than IORQ, which means that IORQ is close to the optimal solution of Problem (4.15).

4.5 Conclusion

In this chapter, the physical layer security in TWRS was studied in the existence of multiple relays and an eavesdropper when each node only has a single antenna and the global CSI is available. We provided two approaches to improve the secure

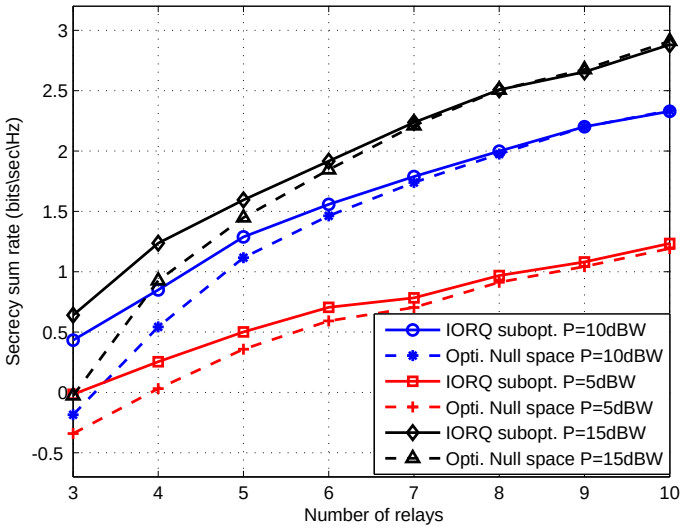

Figure 4.9: Comparison of our solution for null space beamforming and the proposed suboptimal solution (ignoring one Rayleigh quotient) by plotting secrecy sum rate against the number of relays when the total available power is P=10 dBW.

communication rates which are the optimal null space beamforming and IORQ. The optimal null space beamforming vector that has not been solved before was provided. Then an iterative algorithm to enhance the secrecy sum rate by solving the sources powers and beamforming vector problems alternatively was proposed. Another novel suboptimal approach which is called IORQ was proposed. As shown in the simulation results, This approach IORQ outperforms the optimal null space beamforming in case of the number of relays is less than or equal to 8, while at large number of relays, null space beamforming provides a slight improvement over IORQ.

CHAPTER 5

PHYSICAL LAYER SECURITY IN TWRS WHEN CSI IS UNAVAILABLE

5.1 Introduction

In this chapter, we investigate the secure communication in TWRS proposed in the Chapter 4 in case the CSI of the eavesdropper is unavailable. Based on the fact that, in many applications, it is not easy to attain the eavesdropper channel, and in some cases relays and transceivers cannot realize whether there is an eavesdropper or not. In this chapter, we focus on studying the physical layer security under these assumptions. In the second phase, artificial noise is transmitted from the relays to jam the eavesdropper. In other words, relays will work as a jammers to the eavesdropper and a helpers to the legitimate sources. The available

power at the relays is divided into two parts: one part is devoted to amplify and forward the information signals and the rest of the power is devoted to generate an artificial noise to jam the eavesdroppers. In order to reserve the maximum power for jamming the eavesdropper, the optimization problem is formulated so as to minimize the power of the information signal under Qos at both transceivers. We show that the formulated problem is a non-convex QCQP problem, then it can be converted into a SDP with two trace constraints which can be solved by the interior point method. In order to avoid the complexity of the interior point method, we reformulate the problem and propose a novel solution that provides the optimal relays beamforming vector with a significantly lower complexity. We show that in most cases, we can have a closed-form expression of the optimal solution. In addition, our proposed solution can be used for all QCQPs with positive definite objective function and two constraints.

The rest of this chapter is organized as follows; the model of the system is introduced in Section 5.2. In Section 5.3, we present the achievable secrecy sum rate, the problem formulation and proposed solution. Simulation results are given in Section 5.4, and finally the chapter is concluded in Section 5.5.

5.2 System Model

We consider the same system model considered in Chapter 4 with same specifications and constraints except that the CSI of eavesdropper is unavailable.

Therefore, In the second phase, the available power at the relays is divided

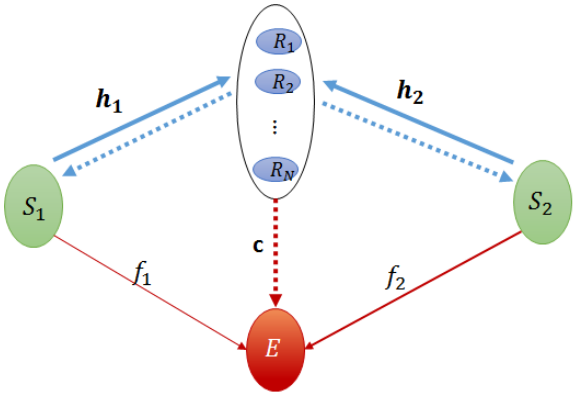

Figure 5.1: System model

into two parts: one part is devoted to amplify the information signal by a complex vector $\mathbf{w}$ and the rest of the power is devoted for the artificial noise to jam the eavesdroppers. As a result, we can write the transmitted signal at the relays as:

$$\mathbf{x}_R = \mathbf{W}\mathbf{y}_R + \mathbf{n}_a, \tag{5.1}$$

where $\mathbf{n}_a$ is the jamming vector or the artificial noise that is designed to interfere the eavesdropper. Vector $\mathbf{n}_a$ is assumed to be designed so that it does not affect the authorized users; i.e., $\mathbf{n}_a$ must be chosen at the null space of the channel vectors $\mathbf{h}_1$ and $\mathbf{h}_2$. In addition, it must be transmitted in all directions to cover all the potential locations of eavesdroppers. The received signals at sources can be expressed as:

$$y_{S1} = \sqrt{P_2}\mathbf{w}^H\mathbf{a}_{12}x_2 + \sqrt{P_1}\mathbf{w}^H\mathbf{a}_{11}x_1 + \mathbf{w}^H\mathbf{H}_1\mathbf{n}_R + \mathbf{n}_a^H\mathbf{h}_1 + n_{S1}, \tag{5.2}$$

$$y_{S2} = \sqrt{P_1}\mathbf{w}^H\mathbf{a}_{12}x_1 + \sqrt{P_2}\mathbf{w}^H\mathbf{a}_{22}x_2 + \mathbf{w}^H\mathbf{H}_2\mathbf{n}_R + \mathbf{n}_a^H\mathbf{h}_2 + n_{S2}. \tag{5.3}$$

In order to eliminate the effect the artificial noise on the legitimate transceivers, we should design the artificial noise such that $\mathbf{n}_a^H \mathbf{h}_1 = \mathbf{n}_a^H \mathbf{h}_2 = 0$. $\sqrt{P_1}\mathbf{w}^H \mathbf{a}_{11} x_1$ in equation (5.2) and $\sqrt{P_2}\mathbf{w}^H \mathbf{a}_{22} x_2$ in equation (5.3) are called the backward self-interference, and can be eliminated if each transmitter knows its instantaneous channel and the beamforming vector $\mathbf{w}$. Therefore, equations (5.2) and (5.3) can be written as:

$$y_{S1} = \sqrt{P_2}\mathbf{w}^H \mathbf{a}_{12} x_2 + \mathbf{w}^H \mathbf{H}_1 \mathbf{n}_R + n_{S_1}, \tag{5.4}$$

$$y_{S2} = \sqrt{P_1}\mathbf{w}^H \mathbf{a}_{12} x_1 + \mathbf{w}^H \mathbf{H}_2 \mathbf{n}_R + n_{S_2}, \tag{5.5}$$

while in the second phase, the eavesdropper can receive a noisy version which can be written as:

$$y_E^{(2)} = \sqrt{P_2}\mathbf{w}^H \mathbf{a}_{c2} x_2 + \sqrt{P_1}\mathbf{w}^H \mathbf{a}_{c1} x_1 + \mathbf{w}^H \mathbf{C}\mathbf{n}_R + \mathbf{c}^H \mathbf{n}_a + n_{e2}. \tag{5.6}$$

Since eavesdropper has two chances to get the information signal from the first and second phase, it can use optimal ratio combining to maximize its SNR and create an equivalent MIMO system. The received signal at the eavesdropper in a vector form can be reformulated as:

$$\mathbf{y}_E = \mathbf{Z}\mathbf{x} + \mathbf{n}_e, \tag{5.7}$$

where $\mathbf{y}_E = \begin{bmatrix} y_E^{(1)} \\ y_E^{(2)} \end{bmatrix}$, $\mathbf{Z} = \begin{bmatrix} \sqrt{P_1} f_1 & \sqrt{P_2} f_2 \\ \sqrt{P_1}\mathbf{w}^H \mathbf{a}_{c1} & \sqrt{P_2}\mathbf{w}^H \mathbf{a}_{c2} \end{bmatrix}$, $\mathbf{n}_e =$

$$\begin{bmatrix} n_{e1} \\ \mathbf{w}^H\mathbf{C}\mathbf{n}_R + \mathbf{c}^H\mathbf{n}_a + n_{e2} \end{bmatrix} \text{ and } \mathbf{s} = \begin{bmatrix} s_1 & s_2 \end{bmatrix}.$$

The information rate at the transceivers are

$$R_{S_1} = \frac{1}{2}\log(1 + \frac{P_2\mathbf{w}^H\mathbf{R}_{12}\mathbf{w}}{\sigma_1^2 + \sigma_R^2\mathbf{w}^H\mathbf{R}_{11}\mathbf{w}}), \tag{5.8a}$$

$$R_{S_2} = \frac{1}{2}\log(1 + \frac{P_1\mathbf{w}^H\mathbf{R}_{12}\mathbf{w}}{\sigma_2^2 + \sigma_R^2\mathbf{w}^H\mathbf{R}_{22}\mathbf{w}}), \tag{5.8b}$$

The information rate at eavesdropper is $R_E = \frac{1}{2}\log\det(\mathbf{I} + \mathbf{Z}\mathbf{Z}^H\mathbf{N}_e^{-1})$, where $\mathbf{N}_e$ is the covariance matrix of the received noise at eavesdropper which is:

$$\mathbf{N}_e = \begin{bmatrix} \sigma_{e1}^2 & 0 \\ 0 & \sigma_{e2}^2 + \sigma_R^2\mathbf{w}^H\mathbf{R}_{cc}\mathbf{w} + \mathbf{n}_a^H\mathbf{R}_{cc}\mathbf{n}_a \end{bmatrix}. \tag{5.9}$$

5.3 Problem Formulation

The optimization problem is formulated based on two criteria: 1) both transceivers have acceptable QoS by assuring that the received SNRs must be greater than a predefined thresholds; and 2) minimize the power devoted for the information signal so that the remain power devoted for the artificial noise is maximized with

a constraint on the relaying power. The optimization problem can be written as:

$$\min_{\mathbf{w}} \quad \mathbf{w}^H(P_1\mathbf{R}_{11} + P_2\mathbf{R}_{22} + \sigma_R^2\mathbf{I}_N)\mathbf{w} \tag{5.10a}$$

$$s.t \quad \frac{P_2\mathbf{w}^H\mathbf{R}_{12}\mathbf{w}}{\sigma_1^2 + \sigma_R^2\mathbf{w}^H\mathbf{R}_{11}\mathbf{w}} \geq \gamma_1, \tag{5.10b}$$

$$\frac{P_1\mathbf{w}^H\mathbf{R}_{12}\mathbf{w}}{\sigma_2^2 + \sigma_R^2\mathbf{w}^H\mathbf{R}_{22}\mathbf{w}} \geq \gamma_2, \tag{5.10c}$$

where γ_1 and γ_2 are predefined thresholds for the information signal to noise ratio at S_1 and S_2, respectively. In general the problem can be expressed as

$$\min_{\mathbf{w}} \quad \mathbf{w}^H(P_1\mathbf{R}_{11} + P_2\mathbf{R}_{22} + \sigma_R^2\mathbf{I}_N)\mathbf{w} \tag{5.11a}$$

$$s.t \quad \mathbf{w}^H(P_1\mathbf{R}_{12} - \sigma_R^2\gamma_1\mathbf{R}_{11})\mathbf{w} \geq \sigma_1^2\gamma_1 \tag{5.11b}$$

$$\mathbf{w}^H(P_1\mathbf{R}_{12} - \sigma_R^2\gamma_2\mathbf{R}_{22})\mathbf{w} \geq \sigma_2^2\gamma_2 \tag{5.11c}$$

Let $\mathbf{G}_0 = (P_1\mathbf{R}_{11} + P_2\mathbf{R}_{22} + \sigma_R^2\mathbf{I}_N)$, $\mathbf{G}_1 = \frac{1}{\sigma_1^2\gamma_1}(P_1\mathbf{R}_{12} - \sigma_R^2\gamma_1\mathbf{R}_{11})$ and $\mathbf{G}_2 = \frac{1}{\sigma_2^2\gamma_2}(P_1\mathbf{R}_{12} - \sigma_R^2\gamma_2\mathbf{R}_{22})$, so we can write (5.11) as

$$\min_{\mathbf{w}} \quad \mathbf{w}^H\mathbf{G}_0\mathbf{w} \tag{5.12a}$$

$$s.t. \quad \mathbf{w}^H\mathbf{G}_1\mathbf{w} \geq \mathbf{1} \tag{5.12b}$$

$$\mathbf{w}^H\mathbf{G}_2\mathbf{w} \geq \mathbf{1}, \tag{5.12c}$$

$\mathbf{G}_0$ can be shown to be a positive definite matrix, while $\mathbf{G}_1$ and $\mathbf{G}_2$ are indefinite matrices. Problem (5.12) can be reformulated as a SDP with rank constraint as

$$\min_{\mathbf{W}} \quad tr(\mathbf{W}\mathbf{G}_0) \tag{5.13a}$$

$$s.t \quad tr(\mathbf{W}\mathbf{G}_1) \geq 1 \tag{5.13b}$$

$$tr(\mathbf{W}\mathbf{G}_2) \geq 1 \tag{5.13c}$$

$$\mathbf{W} \succeq 0, \quad Rank(\mathbf{W}) = 1. \tag{5.13d}$$

The constraint (5.13d) guarantees that the matrix $\mathbf{W}$ can be written as $\mathbf{W} = \mathbf{w}\mathbf{w}^H$. Problem (5.13) is non-convex because the rank constraint of $\mathbf{W}$. In [41], and is shown in Chapter 1, it was shown that if the number of the trace constraints is n, then the global optimal solution matrix $\mathbf{W}$ will have a rank $r \leq \sqrt{n}$. Here, in Problem (5.13), the number of trace constraints is two traces which means that the solution matrix $\mathbf{W}$ will definitely have rank one. Therefore, the optimal beamforming vector $\mathbf{w}$ is the eigenvector related to the maximum eigenvalue of the optimal matrix $\mathbf{W}$. Although, SDP can provide the optimal beamforming vector, it suffers from high complexity, where SDP problems are usually solved via interior point method. Authors in [11] show that the complexity of SDP problem is $O((N+M)^7)$ where M is the number of the trace constraints and N is the row or column dimension of $\mathbf{G}_0$ (number of relays). Hence, here we propose an alternative solution for the SDP problem that provides the optimal beamforming vector with significant decrease in complexity. First, it is direct to show that in Problem (5.13), at least one inequality constraint will be achieved with equality

at optimality. Otherwise, the norm of the beamforming vector can be scaled down to achieve the constraint with equality, which cause a diminution in the objective function.

Theorem 5.1 *If one of the constraints in (5.13) holds with equality, the optimal beamforming vector* $\mathbf{w}^*$ *is either* $\mathbf{w}_1 = \frac{1}{\sqrt{\mathbf{v}_1^H \mathbf{G}_1 \mathbf{v}_1}} \mathbf{v}_1$ *or* $\mathbf{w}_2 = \frac{1}{\sqrt{\mathbf{v}_2^H \mathbf{G}_1 \mathbf{v}_2}} \mathbf{v}_2$, *where* $\mathbf{v}_1 = \mathbf{v}_{max}(\mathbf{G}_0^{-1}\mathbf{G}_1)$, $\mathbf{v}_2 = \mathbf{v}_{max}(\mathbf{G}_0^{-1}\mathbf{G}_2)$.

Proof. The problem in (5.13) is convex since both the objective function and the constraints are convex. It can also be shown that the problem in (5.13) satisfies Slater's condition which states that strong duality holds if there exists a feasible point at which the inequality constraints hold with strict inequalities and the primal optimization problem is convex (details in [42]). Thus, the KKT conditions are necessary and sufficient for a primal-dual point to be optimal. The Lagrangian function of Problem (5.13) is

$$\Gamma = tr(\mathbf{W}\mathbf{G}_0) - tr(\mathbf{W}\mathbf{Q}) - \beta_0 tr(\mathbf{W}\mathbf{G}_1) - \beta_1 tr(\mathbf{W}\mathbf{G}_2) + \beta_0 + \beta_1, \qquad (5.14)$$

where $\beta_0 \geq 0, \beta_1 \geq 0$ and $\mathbf{Q} \succeq 0$ are the Lagrangian dual variables. The KKT conditions are:

$$\frac{d\Gamma}{d\mathbf{W}} = \mathbf{G}_0 - \mathbf{Q}^* - \beta_0^*\mathbf{G}_1 - \beta_1^*\mathbf{G}_2 = 0 \tag{5.15a}$$

$$tr(\mathbf{W}^*\mathbf{G}_1) - 1 \geq 0 \tag{5.15b}$$

$$tr(\mathbf{W}^*\mathbf{G}_2) - 1 \geq 0 \tag{5.15c}$$

$$tr(\mathbf{W}^*\mathbf{Q}) = 0 \tag{5.15d}$$

$$\beta_0^* tr(\mathbf{W}^*\mathbf{G}_1) - \beta_0^* = 0 \tag{5.15e}$$

$$\beta_1^* tr(\mathbf{W}^*\mathbf{G}_2) - \beta_1^* = 0 \tag{5.15f}$$

$$\mathbf{W}^* \succeq 0, \quad \mathbf{Q}^* \succeq 0 \quad \beta_0^* \geq 0 \quad \beta_1^* \geq 0. \tag{5.15g}$$

From KKT conditions, the dual optimization problem can be written as

$$\max_{\beta_0,\beta_1} \quad \beta_0 + \beta_1 \tag{5.16a}$$

$$s.t. \quad \mathbf{G}_0 - \beta_0\mathbf{G}_1 - \beta_1\mathbf{G}_2 \succeq 0, \tag{5.16b}$$

$$\beta_0 \geq 0, \beta_1 \geq 0. \tag{5.16c}$$

Without loss of generality, assume that (5.13c) does not hold with equality which means that β_1^* must be zero to satisfy (5.15f). Therefore, Problem (5.16) can be

written as

$$\max_{\beta_0,\beta_1} \quad \beta_0 \tag{5.17a}$$

$$s.t. \quad \mathbf{G}_0 - \beta_0 \mathbf{G}_1 \succeq 0, \tag{5.17b}$$

$$\beta_0 \geq 0. \tag{5.17c}$$

It can be shown that when $tr(\mathbf{W}^*\mathbf{G}_1) < tr(\mathbf{W}^*\mathbf{G}_2)$, then (5.13b) holds with equality while (5.13c) does not, and vice versa. Furthermore, at optimality both the objective function of the primal and dual optimization problems are equal, β_0^*=$tr(\mathbf{W}^*\mathbf{G}_0)$=$\frac{tr(\mathbf{W}^*\mathbf{G}_0)}{tr(\mathbf{W}^*\mathbf{G}_1)}$=$\frac{\mathbf{w}^{*H}\mathbf{G}_0\mathbf{w}^*}{\mathbf{w}^{*H}\mathbf{G}_1\mathbf{w}^*}$. In addition, from the constraint (5.17b) we have $\mathbf{I} \succeq \beta_0^*\mathbf{G}_0^{-1}\mathbf{G}_1$, and hence $\frac{1}{\beta_0^*}\mathbf{I} \succeq \mathbf{G}_0^{-1}\mathbf{G}_1$,which can be written as $\frac{1}{\beta_0^*} \geq \lambda_{max}(\mathbf{G}_0^{-1}\mathbf{G}_1)$. This means that the maximum value of β_0^* is $\frac{1}{\lambda_{max}(\mathbf{G}_0^{-1}\mathbf{G}_1)}$. Hence,

$$\frac{\mathbf{w}^{*H}\mathbf{G}_1\mathbf{w}^*}{\mathbf{w}^{*H}\mathbf{G}_0\mathbf{w}^*} = \frac{1}{\beta_0^*} = \lambda_{max}(\mathbf{G}_0^{-1}\mathbf{G}_1). \tag{5.18}$$

The optimal beamforming vector that satisfies (5.18) is $\mathbf{v}_{max}(\mathbf{G}_0^{-1}\mathbf{G}_1)$ =$\mathbf{v}_1$. But we have to scale the solution vector to satisfy the constraints in problem (5.13). Note that the scaling does not affect (5.18). Hence, we have $\mathbf{w}^*$=$\frac{1}{\sqrt{\mathbf{v}_1^H\mathbf{G}_1\mathbf{v}_1}}\mathbf{v}_1$ aiming to have the constraint (5.13b) active while the (5.13c) strict. Similarly, if (5.13c) holds with equality while (5.13b) does not, it can be shown that the solution vector is $\mathbf{w}^*$=$\frac{1}{\sqrt{\mathbf{v}_2^H\mathbf{G}_1\mathbf{v}_2}}\mathbf{v}_2$. Briefly, the optimal beamforming vector is $\mathbf{w}_1$ if (5.13b) holds with equality, whereas the solution vector is $\mathbf{w}_2$ if (5.13c) holds with equality. ∎

Now, two questions should be raised here: 1) How would we determine which constraint will hold with equality? 2) What is the solution vector if both constraints hold with equality?. To answer the first question we consider three cases:

- Case 1: If one of the solution vectors is feasible while the other is not, select the feasible one.
- Case 2: If both of them are feasible, select the vector that minimizes the objective function of Problem (5.13) more than the other.
- Case 3: If both of them are infeasible (which rarely occurs), it means that at optimality both constraints hold with equality. This can be proved from the dual problem (5.16). Both constraints hold with equality means that $\beta_0 > 0$ and $\beta_1 > 0$, which means that neither $\mathbf{w}_1$ nor $\mathbf{w}_2$ can be a solution for Problem (5.12).

In Cases 1 and 2, we have a closed-form solution to Problem (5.13). Despite the rare occurrence of the third case, we propose another solution, other than the SDP approach to avoid the complexity, which also provides the answer for the second question. Here, we provide a solution for the problem in (5.13) in case of both constraints hold with equality. Problem (5.13) can be written as

$$\min_{\mathbf{W}} \quad tr(\mathbf{W}\mathbf{G}_0) \tag{5.19a}$$

$$s.t \quad tr(\mathbf{W}\mathbf{G}_1) = 1 \tag{5.19b}$$

$$tr(\mathbf{W}\mathbf{G}_2) = 1 \tag{5.19c}$$

$$\mathbf{W} \succeq 0, \tag{5.19d}$$

Problem (5.19) is similar to the Problem (2.17) that is solved in Chapter 2. Therefore, the proposed Algorithm (2.1) can be used to provide the optimal solution of Problem (5.19) efficiently.

Therefore, the algorithm to solve Problem (5.12) to obtain $\mathbf{w}^*$ is

---

Algorithm 5.1 Finding the optimal solution of Problem (5.12).

---

1. find $\mathbf{w}_1=\frac{1}{\sqrt{\mathbf{v}_1^H\mathbf{G}_1\mathbf{v}_1}}\mathbf{v}_1$, and $\mathbf{w}_2 = \frac{1}{\sqrt{\mathbf{v}_2^H\mathbf{G}_2\mathbf{v}_2}}\mathbf{v}_2$.
2. If both $\mathbf{w}_1$ and $\mathbf{w}_2$ are feasible, select the vector that minimizes the objective function of problem (5.13) more than the other.
3. If one of the solution vectors is feasible while the other is not, select the feasible one
4. If both of them are infeasible (which rarely occurs) use Algorithm 2.1 to have the optimal vector.

5.4 Simulation Results

Here, simulation results are introduced to demonstrate the effectiveness of the proposed physical layer security algorithms. In each simulation result, we generate each channel randomly as independent complex Gaussian random variables with zero mean and unit variance. All SDP problems are solved efficiently using interior point method provided by Matlab CVX toolbox [3]. We obtain the results by averaging over 5000 Monte Carlo channel realization. In Fig. 5.2, it is obvious that the secrecy sum rate increases with the maximum available power at the relays until some point where the secrecy sum rate saturates; i.e., there is a limit for the secrecy sum rate despite we have a boundless relays power. This is because

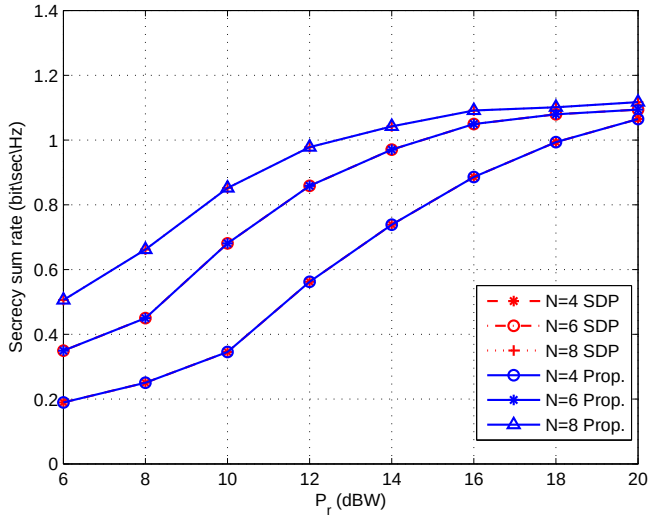

Figure 5.2: Secrecy sum rate against the total available power at relays with various number of relays, since $\gamma_1 = \gamma_2 = 10dB$ and transceivers power $P_1 = P_2 = 12dBW$.

the required signal to noise ratios at transceivers (γ_1 and γ_2) are fixed, while the information rate at the eavesdropper goes to zero with infinite artificial noise power. It is also seen that increasing the number of relays improves the physical layer security in the system. The results in Fig. 5.2 show that for different number of relays and different total relays power levels, both SDP approach and our proposed algorithm provide the same optimal solution vector and the same secrecy sum rate.

In Fig. 5.3 we compare the computational complexity of SDP approach and our approach in terms of the execution time. We plot the average percentage ratio of execution time spent by the proposed solution with respect to the SDP approach. It is shown that our algorithm provides substantially less computational complexity than the SDP approach where, on average, it consums only 0.57% of the time consumed by SDP.

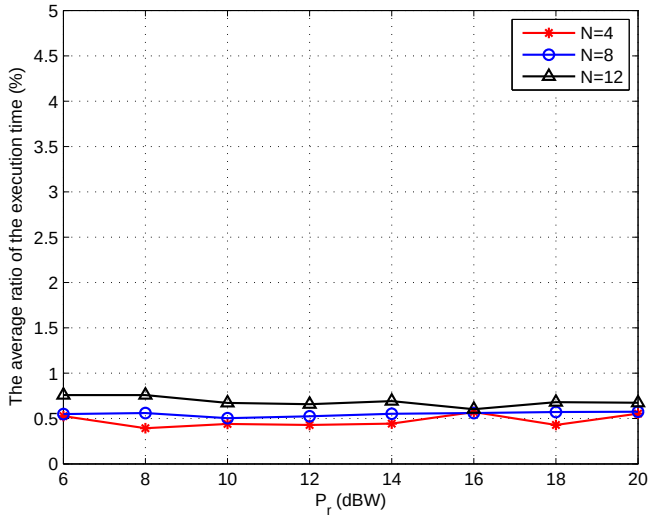

Figure 5.3: The average ratio of execution time spent by implementing our Algorithm 5.1 with relative to SDP approach against maximum available power at relays, N=4, N=8, N=12.

In Fig. 5.4, a special case of our problem is implemented where it is assumed that the QoS in both transceivers must satisfy, with equality, the exact SNR. In other words, we compare the SDP (5.19) to the proposed Algorithm 1. Similar to Fig. 5.2, the results in Fig. 5.4 show that for different number of relays and different total relays power levels, both the SDP approach and our proposed algorithm provide the same optimal solution vector and the same secrecy sum rate.

In Fig. 5.5, when both constraints must hold with equality, we compare the computational complexity of the SDP approach and Algorithm 1 in terms of the execution time. We plot the average ratio of execution time consumed by the proposed solution with respect to the SDP approach. It is shown that our algorithm provides substantially less complexity computational complexity than the SDP approach where, on average, consumes about 1.13%, 2.15%, and 3.41%

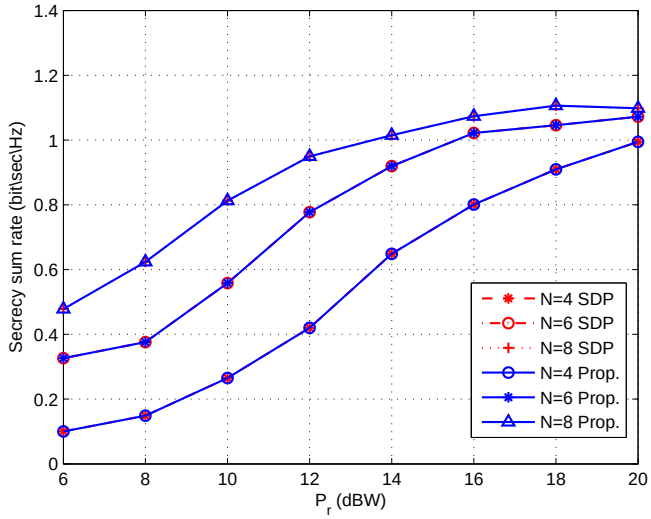

Figure 5.4: Comparison of SDP problem when both constraints hold with equality and Algorithm 2.1, since $\gamma_1 = \gamma_2 = 10dB$ and transceivers power $P_1 = P_2 = 12dBW$

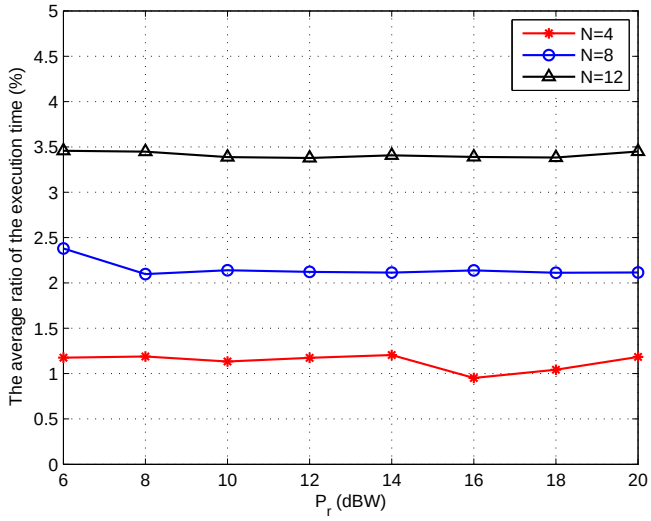

Figure 5.5: The average ratio of execution time spent by implementing our Algorithm 1 with relative to SDP approach when both constraints satisfied with equality versus maximum available power at relays with different number of relays; N=4, N=8, N=12.

of the time consumed by SDP in case of 4, 8, and 12 relays, respectively.

5.5 Conclusion

In this chapter, we considered a TWRS with one eavesdropper, where artificial noise was used to maximize the secrecy rate. In order to maximize the artificial noise power, we studied the problem of minimizing the information signal power. An efficient algorithm to minimize the power was proposed where, in most cases a closed-form expression of the optimal solution is provided. It was shown that the proposed algorithm provides the same optimal solution that can be achieved using SDP, but with dramatically reduced computational complexity.

CHAPTER 6

CONCLUSION AND FUTURE WORK

In this chapter, the contribution of this thesis is summarized including the contribution of the physical layer security in OWRS, and in TWRS with and without CSI. Furthermore, some interesting topics in the scope of physical layer security in relay networks are suggested as future research.

6.1 Summary of contributions

Here, we conclude the contribution of this thesis. The physical layer security in OWRS was studied in two chapters. In Chapter 2, the power of relays minimization under secrecy rate constraint was formulated. It was shown that the problem is a nonconvex QCQP problem where it is not easy to solve it. A novel solution was proposed to solve the QCQP problem which guarantee the optimal solution with substantial low complexity. It was also proved that, in the relaying power

minimization problem under QoS constraints, the optimal value of the source power is its maximum available power.

Then, maximizing the product of two RQs problem was solved. This problem has been considered in the previous work as a difficult problem where suboptimal solutions have been proposed. Therefore, an efficient algorithm was provided that guarantee the optimal solution of maximizing the product of two RQs aiming to:

1. Maximize the secrecy rate in OWRS as illustrated in Chapter 3.

2. Maximize the secrecy sum rate in TWRC when the null space beamforming is applied as shown in Chapter 4.

3. Find a suboptimal solution for the secrecy sum rate maximization in TWRS which provided a remarkable improvement in secrecy sum rate as shown in the simulation results of Chapter 4.

This problem of optimizing the product of the two RQs was first converted from N-dimensional search to one dimensional search where a SDP has to be solved in each iteration. Then the problem was significantly simplified by converting it from a series of SDPs to a series of a generalized eigenvalue problems. Finally, an efficient algorithm was proposed to find the optimal beamforming vector.

Additionally, in Chapter 4, it was shown in TWRS that eliminating the full information for the eavesdropper may degrade the information rates at the transceivers especially in case of having a small number of relay nodes and low power, whereas we can allow some of the information signal to be received by

the eavesdropper as long as it is at noise level and exploit that in enhancing the SNR at the transceivers. We provided an efficient solution for how to exploit the allowed eavesdropper information rate to enhance the information rates at the transceivers. This was shown by simulation results where a significant improvement in secrecy sum rate has been achieved.

Furthermore, a novel approach to solve the QCQP with two constraints and positive definite matrix at the objective function was proposed. As shown in Chapter 2 and Chapter 5, this approach has significantly decreased the complexity of solving the QCQP problems compared to SDP approach. This approach can also be applied to tackle many problems that we are intending to consider as a future work.

6.2 Future work

Although we provided an efficient algorithm to solve QCQP problems, it is required to extend the proposed algorithm to tackle the QCQPs when the trace constraints are more than two traces. This will grant us the capability to utilize the proposed algorithms in solving several problems in this area such as:

1. Minimizing the total power under individual information rate constraints in TWRS at the transceivers and the eavesdropper.

2. Maximizing the SNR of the destination in OWRS with the existence of multiple eavesdroppers. In other words, maximize the SNR of the destination under a constraints on the SNR of the eavesdroppers.

In TWRS, although we provide the optimal null space beamforming that prevents the eavesdropper to receive a version of the transmitted signal through the second phase, the eavesdropper still has a chance to receive a version during the first phase. This is encouraging to study the selection of some relays to work as a jammers in order to confuse the eavesdropper in both phases. This problem will be formulated to find the optimal number of jammers and the optimal power of jamming signal.

It is also recommended to study the physical layer security in a hybrid relaying system. This system is a mixed of TWRS and OWRS which has not been proposed before, where it can be built by adding one legitimate destination to the TWRS.

REFERENCES

[1] A. Mukherjee, S. A. Fakoorian, J. Huang, A. L. Swindlehurst *et al.*, "Principles of physical layer security in multiuser wireless networks: A survey," *Communications Surveys & Tutorials, IEEE*, vol. 16, no. 3, pp. 1550–1573, 2014.

[2] J. F. Sturm, "Using sedumi 1.02, a matlab toolbox for optimization over symmetric cones," *Optimization methods and software*, vol. 11, no. 1-4, pp. 625–653, 1999.

[3] M. Grant and S. Boyd, "Cvx: Matlab software for disciplined convex programming."

[4] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 24, no. 3, pp. 339–348, 1978.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas i: The misome wiretap channel," *Information Theory, IEEE Transactions on*, vol. 56, no. 7, pp. 3088–3104, 2010.

[6] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Qos-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," pp. 1202–1216, 2011.

[7] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-part ii: The mimome wiretap channel," *Information Theory, IEEE Transactions on*, vol. 56, no. 11, pp. 5515–5532, 2010.

[8] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *Signal Processing, IEEE Transactions on*, vol. 58, no. 3, pp. 1875–1888, 2010.

[9] J. Zhang and M. C. Gursoy, "Relay beamforming strategies for physical-layer security," in *Information Sciences and Systems (CISS), 2010 44th Annual Conference on*. IEEE, 2010, pp. 1–6.

[10] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *Signal Processing, IEEE Transactions on*, vol. 60, no. 7, pp. 3532–3545, 2012.

[11] Y. Yang, C. Sun, H. Zhao, H. Long, and W. Wang, "Algorithms for secrecy guarantee with null space beamforming in two-way relay networks," *Signal Processing, IEEE Transactions on*, vol. 62, no. 8, pp. 2111–2126, 2014.

[12] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal, The*, vol. 54, no. 8, pp. 1355–1387, 1975.

[13] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wire-tap channel," *Information Theory, IEEE Transactions on*, vol. 24, no. 4, pp. 451–456, 1978.

[14] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *Information Theory, IEEE Transactions on*, vol. 54, no. 10, pp. 4687–4698, 2008.

[15] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on.* IEEE, 2007, pp. 1296–1300.

[16] P. Parada and R. Blahut, "Secrecy capacity of simo and slow fading channels," in *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on.* IEEE, 2005, pp. 2152–2155.

[17] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the gaussian mimo wire-tap channel: The 2-2-1 channel," *Information Theory, IEEE Transactions on*, vol. 55, no. 9, pp. 4033–4039, 2009.

[18] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference*, vol. 62, no. 3. IEEE; 1999, 2005, p. 1906.

[19] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 6, pp. 2180–2189, 2008.

[20] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for miso multi-eves secrecy rate maximization," *Signal Processing, IEEE Transactions on*, vol. 61, no. 10, pp. 2704–2717, 2013.

[21] O. Simeone and P. Popovski, "Secure communications via cooperating base stations," *Communications Letters, IEEE*, vol. 12, no. 3, pp. 188–190, 2008.

[22] L. Lai and H. E. Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *Information Theory, IEEE Transactions on*, vol. 54, no. 9, pp. 4005–4019, 2008.

[23] J. Kim, A. Ikhlef, and R. Schober, "Combined relay selection and cooperative beamforming for physical layer security," *Communications and Networks, Journal of*, vol. 14, no. 4, pp. 364–373, 2012.

[24] J. Li, A. P. Petropulu, and S. Weber, "Optimal cooperative relaying schemes for improving wireless physical layer security," *arXiv preprint arXiv:1001.1389*, 2010.

[25] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. Ching, "Cooperative secure beamforming for af relay networks with multiple eavesdroppers," *Signal Processing Letters, IEEE*, vol. 20, no. 1, pp. 35–38, 2013.

[26] M. Jilani and T. Ohtsuki, "Joint svd-gsvd precoding technique and secrecy capacity lower bound for the mimo relay wire-tap channel," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, no. 1, pp. 1–8, 2012.

[27] S. A. A. Fakoorian *et al.*, "Solutions for the mimo gaussian wiretap channel with a cooperative jammer," *Signal Processing, IEEE Transactions on*, vol. 59, no. 10, pp. 5013–5022, 2011.

[28] J. Wang *et al.*, "Cooperative jamming in mimo ad-hoc networks," in *Signals, Systems and Computers, 2009 Conference Record of the Forty-Third Asilomar Conference on*. IEEE, 2009, pp. 1719–1723.

[29] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *Communications Letters, IEEE*, vol. 16, no. 10, pp. 1628–1631, 2012.

[30] C. Wang, H.-M. Wang, and X.-G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *Wireless Communications, IEEE Transactions on*, vol. 14, no. 2, pp. 589–605, 2015.

[31] C. Wang, H. Wang, D. Ng, X. Xia, and C. Liu, "Joint beamforming and power allocation for secrecy in peer-to-peer relay networks."

[32] R. Zhang, L. Song, Z. Han, B. Jiao, and M. Debbah, "Physical layer security for two way relay communications with friendly jammers," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*. IEEE, 2010, pp. 1–6.

[33] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2735–2751, 2008.

[34] H.-M. Wang, Q. Yin, and X.-G. Xia, "Improving the physical-layer security of wireless two-way relaying via analog network coding," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*. IEEE, 2011, pp. 1–6.

[35] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *Information Forensics and Security, IEEE Transactions on*, vol. 8, no. 12, pp. 2007–2020, 2013.

[36] R. Zhang, L. Song, Z. Han, B. Jiao, and M. Debbah, "Physical layer security for two way relay communications with friendly jammers," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*. IEEE, 2010, pp. 1–6.

[37] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 1, pp. 310–320, 2012.

[38] H. Cui, R. Zhang, L. Song, and B. Jiao, "Performance analysis of bidirectional relay selection with imperfect channel state information," *arXiv preprint arXiv:1112.2374*, 2011.

[39] Z.-Q. Luo, W.-k. Ma, A. M.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *Signal Processing Magazine, IEEE*, vol. 27, no. 3, pp. 20–34, 2010.

[40] Q. Li, Q. Zhang, and J. Qin, "A special class of fractional qcqp and its applications on cognitive collaborative beamforming," pp. 2151–2164, 2014.

[41] Y. Huang and D. P. Palomar, "Rank-constrained separable semidefinite programming with applications to optimal beamforming," *Signal Processing, IEEE Transactions on*, vol. 58, no. 2, pp. 664–678, 2010.

[42] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[43] F. J. Solis and R. J.-B. Wets, "Minimization by random search techniques," *Mathematics of operations research*, vol. 6, no. 1, pp. 19–30, 1981.

[44] A. Goldsmith, *Wireless Communications*. New York, NY, USA: Cambridge University Press, 2005.

[45] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secure broadcasting," in *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*. IEEE, 2010, pp. 1–6.

[46] A. Mukherjee *et al.*, "Securing multi-antenna two-way relay channels with analog network coding against eavesdroppers," in *Signal Processing Advances in Wireless Communications (SPAWC), 2010 IEEE Eleventh International Workshop on*. IEEE, 2010, pp. 1–5.

[47] V. Havary-Nassab, S. Shahbazpanahi, and A. Grami, "Optimal distributed beamforming for two-way relay networks," *Signal Processing, IEEE Transactions on*, vol. 58, no. 3, pp. 1238–1250, 2010.

[48] A. Charnes and W. W. Cooper, "Programming with linear fractional functionals," *Naval Research logistics quarterly*, vol. 9, no. 3-4, pp. 181–186, 1962.

[49] R. Zhang, Y.-C. Liang, C. C. Chai, and S. Cui, "Optimal beamforming for two-way multi-antenna relay channel with analogue network coding," *Selected Areas in Communications, IEEE Journal on*, vol. 27, no. 5, pp. 699–712, 2009.

[50] L. Vandenberghe and S. Boyd, "Semidefinite programming," *SIAM review*, vol. 38, no. 1, pp. 49–95, 1996.

Vitae

- **Name:** Mohanad Ali Abdulwahid Obeed
- **Nationality:** Yemeni
- **Date of Birth:** 21/03/1986
- **Email:** *g201106250@kfupm.edu.sa*
- **Permenant Address:** Taiz, Yemen

- **MSc.** Degree in Telecommunication Engineering, KFUPM, Dhahran, KSA, 2015.
- **BACHELOR'S DEGREE** Communication and Computer Engineering (Communication Sector), TAIZ UNIVERSITY, 2008.
- **Research Field of Interest:** Wireless Communications, Cooperative Communication, Physical Layer Security , Convex Optimization, Game Theory.
- **Publications:**
  - Mohanad Obeed, Wessam Mesbah, "An Efficient Physical Layer Security Algorithm for Two-Way Relay Systems", *IEEE Conf. Wireless Commun. and Netwo. (WCNC),* 2016.